NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EXPEDITIONARY MOBILE OPERATIONS CENTER (EMOC)

by

Jose Gonzalez

September 2014

Thesis Advisor:	Douglas J. MacKinnon
Second Reader:	Albert Barreto III

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
EXPEDITIONARY MOBILE OPERATIONS CENTER (EMOC)

5. FUNDING NUMBERS

6. AUTHOR: Jose Gonzalez

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

This research explores a viable solution to the U.S. Marine Corps' (USMC) communications gap at the tactical edge. The aim is to leverage commercial-off-the-shelf (COTS) technology to provide a combat operations center (COC) like communication architecture to small units operating in austere environments. The proposed architecture required must be lightweight, energy efficient, and allow greater mobility through a reduced footprint and energy consumption. By reducing the energy required for unit communications, this theoretical architecture decreases fuel needs, leading to a reduction in logistical-supply requirements.

The emergency operational center (EOC) architectural concept is examined as an example of virtualized technology to determine how such an architecture might satisfy USMC requirements. Server virtualization, hastily formed networks, the functionality of software and hardware in a virtual environment, and the original concept of the EOC architecture are explored. Expeditionary considerations and Marine Air Ground Task Force command-and-control (C2) characteristics are also considered, along with current communication architectures, comparing capabilities, weight, and power consumption to determine a baseline for future C2 technology. Finally, the interoperability and security of the EOC are discussed in relation to software and hardware used by the USMC.

14. SUBJECT TERMS: Cloud Computing, Virtualization, Virtual Environment, Virtual Machine, Thin Client, Zero Client, Virtual Security, Virtual Infrastructure, Trusted Enclave, Security Vulnerabilities, Infrastructure attacks, Hyperjacking, Virtual Machine Jumping, on-the-move (OTM) communication, Network-on-the-move (NOTM).

15. NUMBER OF PAGES 127

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EXPEDITIONARY MOBILE OPERATIONS CENTER (EMOC)

Jose Gonzalez
Captain, United States Marine Corps
B.S., University of the Pacific, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2014

Author: Jose Gonzalez

Approved by: Douglas J. MacKinnon, Ph.D.
Thesis Advisor

Albert Barreto III
Second Reader

Dan Boger, Ph.D.
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research explores a viable solution to the U.S. Marine Corps' (USMC) communications gap at the tactical edge. The aim is to leverage commercial-off-the-shelf (COTS) technology to provide a combat operations center (COC) like communication architecture to small units operating in austere environments. The proposed architecture required must be lightweight, energy efficient, and allow greater mobility through a reduced footprint and energy consumption. By reducing the energy required for unit communications, this theoretical architecture decreases fuel needs, leading to a reduction in logistical-supply requirements.

The emergency operational center (EOC) architectural concept is examined as an example of virtualized technology to determine how such an architecture might satisfy USMC requirements. Server virtualization, hastily formed networks, the functionality of software and hardware in a virtual environment, and the original concept of the EOC architecture are explored. Expeditionary considerations and Marine Air Ground Task Force command-and-control (C2) characteristics are also considered, along with current communication architectures, comparing capabilities, weight, and power consumption to determine a baseline for future C2 technology. Finally, the interoperability and security of the EOC are discussed in relation to software and hardware used by the USMC.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAV	Amphibious Assault Vehicle
AD	active directory
AES	Advanced Encryption Standard
AO	area of operation
ATH	at-the-halt
AN/PRC	Army/Navy portable radio configuration
ANW	Adaptive Networking Wideband Waveform
BN	battalion
BGAN	Broadband Global Area Network
BLOS	beyond-line-of-sight
CAPSET	capabilities set
CCI	controlled cryptographic item
CENTRIX	combined enterprise regional information exchange
CIA	confidentiality, integrity & availability
CMC	Commandant of the Marine Corps
COC	combat operation center
COCOM	combatant commander
COMSEC	communication security
CONUS	continental United States
COP	combat outpost
COTS	commercial-off-the-shelf
CPOF	Command Post of the Future
C2	command & control
C2PC	command & control personal computer
DHCP	dynamic host configuration protocol
DNS	domain name server
DOD	Department of Defense
DSU	digital switching units
EOC	emergency operations center
EMOC	expeditionary mobile operations center

EMW	expeditionary maneuver warfare
FRC	first responder community
FOB	Forward Operating Base
Gbps	gigabits per sec
GB	gigabits
GIG	Global Information Grid
GRE	generic routing encapsulation
HADR	humanitarian assistance and disaster relief
HAIPE	High Assurance Internet Protocol Encryption
HDD	hard disk drive
HFN	hastily formed network
HMMWV	Highly Mobile Multipurpose Wheeled Vehicle
HQ	headquarters
IP	Internet protocol
JTCW	Joint Tactical Common Workstation
KVM	keyboard, video & mouse
L-L&C	lift – lift & carry
M	model
MAG	Marine Air Group
MAGTF	Marine Air Ground Task Force
MARCORSYSCOM	Marine Corps Systems Command
M-ATV	Mine-Resistant Ambush protected All-Terrain Vehicle
MCDP	Marine Corps Doctrinal Publication
MCO	Marine Corps Order
mIRC	Microsoft Internet Relay Chat
MPG	miles per gallon
MRAP	Mine-Resistant Ambush Protected
MTVR	Medium Tactical Vehicle Replacement
MWSS	Marine Wing Support Squadrons
NAT-T	network address translation traversal
NCW	Net Centric Warfare
NIOSH	National Institute for Occupational Safety and Health

NIPRNET	non-classified Internet protocol router network
NIST	National Institute of Science & Technology
NGO	non-governmental organization
NOTM	networking-on-the-move
NSA	National Security Agency
OCONUS	outside the continental United States
OGA	other government agencies
OS	Operating System
OSHA	Occupational Safety and Health Administration
OTM	on the move
OTH	over-the-horizon
PCMCIA	Personal Computer Memory Card International Association
PDU	power distribution unit
PoE	Power over Ethernet
POP-V	Point of Presence vehicle
RMOD	radio module
SA	situational awareness
SAN	storage area network
SATCOM	satellite communication
SECNET	secure network
SIPRNET	secure Internet protocol router network
SOF	Special Operation Forces
SoS	system of systems
SOQH	SATCOM-on-the-quick-halt
SP	Special Publication
SSD	solid-state drive
S&TSP	Science & Technology Strategic plan
SK	staff kit
SVK	staff vehicle kit
SWAN	support side area network
SWLAN	secure wireless local area network

TB	terabytes
TDS	Tactical Data Systems
TEP	Tactical Entry Point
TM	Technical Manual
TOCNET	Tactical Operations Center Intercommunications
TS/SCI	top secret/sensitive compartmented information
UPS	uninterrupted power supply
UNS	universal needs statement
USMC	United States Marine Corps
VDI	virtual desktop infrastructure
VHF	very high frequency
VLAN	virtual local area network
VM	virtual machine
VMS	Virtualization Management System
VoIP	Voice over Internet protocol
VPN	Virtual Private Network
VSAT-L	very-small-aperture-terminal-Large
W/h	watts per hour

I. INTRODUCTION

A. EXPEDITIONARY MOBILE-OPERATIONS CENTER (EMOC)

The U.S. Marine Corps (USMC) operates in austere environments throughout the world and must communicate using organic assets. Each element must be able to communicate at the tactical edge. Current efforts to communicate within the tactical edge remain difficult because of marginal technology in the areas of voice and data communication, mobility, and energy efficiency.

The USMC has identified deficiencies in its communication systems and seeks ways to increase the reliability of voice and data transmission, enhance mobility, and exploit alternative-energy sources, thus simplifying logistics for forward-deployed units. Units in battle must be able to set up and expand networks rapidly, especially when required to engage, pack up immediately, and move to another position. Units operating a forward combat operations center (COC) with a small ad-hoc network also require reliable, portable, and energy-thrifty systems. The military's current equipment set makes it difficult for these small units to move quickly while maintaining the full communication capabilities of the main COC, and capability is often sacrificed to maneuverability.

During a deployment to Afghanistan in 2010, while traveling to a number of small Forward Operating Bases (FOBs) occupied by platoon-size elements, we observed that the communications of these small units were limited to voice and data messaging (text messaging via VHF single-channel radio). These constraints might be mitigated under today's technology. The USMC's directives for cloud computing calls for FOB support as follows:

- Facilitate secure communications and IT services that provide robust, near-real-time access to mission-critical data, information, and knowledge.
- Provide a net-centric information environment that enables access to rear echelon data resources at the battalion level and below.

- Enable dispersed operations in a non-linear battle space over greater distances by providing more information with fewer deployed resources.

- Implement virtualization technologies to reduce footprint and energy requirements and increase the speed of network implementation (Anderson, 2012, p. 4).

With the advent of virtual machines and wireless technologies, it is possible for small units operating in a FOB miles from headquarters or Special Operations Forces (SOF) in austere environments to capitalize on all COC communications capabilities while maintaining maneuverability and meeting the USMC's vision of cloud-computing support of forward-operating units. In addition, with the incorporation of virtual machines, section leaders and commanders can potentially leave the COC and still pull or push information to higher headquarters. Wireless technology can potentially enable units to maneuver within an area and still connect to their network. This research shows how reengineering the Naval Postgraduate School's emergency operations center (EOC) "in-a-box" architecture would allow the military to take advantage of a communication system that integrates virtual-machine technology into a hastily formed network to support military operations. The reengineering of the EOC-in-a-box is dubbed the expeditionary mobile operations center (EMOC).

B. RESEARCH QUESTION

The following questions are explored in this research.

1. How can the current EOC-in-a-box architecture be modified to reduce weight, improve maneuverability, and still provide the security and C2 capabilities needed to bridge the communications gap?

2. How can the EOC-in-a-box's energy-efficiency plan be modified to reduce the logistical burden associated with C2?

C. BENEFITS

After over a decade of fighting the insurgency in Afghanistan, the USMC is determined to return to its expeditionary roots by enhancing C2 capabilities from the headquarters level down to the smallest units. To transition from a force accustomed to maintaining a large footprint on the battlefield to one that can maneuver swiftly without losing C2 capabilities, the USMC needs to exploit today's commercial technology.

New technologies can allow the USMC to continue operating in austere environments without sacrificing C2 capabilities, by reducing unit dependency on fossil fuels and lightening the Marine Air Ground Task Force (MAGTF)—improving maneuverability and communications at all levels while supporting its ability to function in the irregular-warfare environment. The use of virtual machines is extremely promising toward this progress. By reducing the size, weight, and fuel consumption of communication assets for the USMC, virtual machines could render units more maneuverable and less dependent on fuel, and the logistical support that goes with it, thus making the USMC more expeditionary and closing the communications gap identified.

D. RESEARCH DESIGN AND METHODOLOGY

This research evaluates current and developing communications systems that incorporate virtual-machine technology to evaluate the feasibility of deploying virtualized technology to the tactical edge. These evaluations are based on quantitative data measuring weight, power consumption, and compatibility with current USMC software and hardware.

E. THESIS ORGANIZATION

1. Chapter II: Technology and Definitions

Chapter II provides a general understanding of the background, fundamentals, and capabilities of leveraging virtualization technology in mobile command-and-control in austere environments. It introduces server virtualization,

hastily formed networks (HFN), how software and hardware function in a virtual environment, and the original EOC concept.

2. Chapter III: Current USMC C2 Technology

Chapter III provides information on expeditionary considerations and MAGTF C2 characteristics, analyzing current and developing Marine Corps communication architectures and comparing their capabilities, weight, and power consumption to determine a baseline for future C2 technology.

3. Chapter IV: Analysis and Application

The interoperability and security of the EOC in relation to specific software and hardware used by the USMC is addressed in Chapter IV. Experiments are conducted on the original and follow-up EOC model and an EMOC model is proposed to fill communication gaps.

4. Chapter V: Conclusion and Recommendations

Chapter V examines findings according to the research questions posed in Chapter I, which are broken down and answered based on the information discovered. A way forward is recommended and areas for further research are suggested.

II. BACKGROUND TECHNOLOGY AND DESCRIPTIONS

A. BACKGROUND

Communication is imperative in combat, and equally important with the need to share information among troops and allies is the need for operational secrecy. Thus, it is important to maintain alternative lines of communication and networks among government forces and allies. In recent years, the convergence of data, voice, and multimedia over the network, coupled with continual improvement in network capacity and reliability, has supported a wide range of communication applications. Examples range from general-purpose communication, such as voice-over-Internet protocol (VoIP) telephony and video, to other networks, such as the non-classified Internet protocol router network (NIPRNET), secret Internet protocol router network (SIPRNET), combined enterprise regional information exchange (CENTRIX), and the NATO secret network.

Through its Science and Technology Strategic Plan (S&TSP) (2012), the USMC has established priorities for promoting new technologies, based on the USMC expeditionary maneuver warfare (EMW) capabilities list and subsequent solutions-planning directive, which aimed at closing the capability gaps identified in the EMW, including communications gaps. Improving voice and data communication, enhancing command mobility, and reducing the logistical requirements associated with supporting a COC, while at the same time maintaining the ability to communicate over different networks have been designated a priority (USMC, 2012). Lacking these capabilities, it is difficult for commanders to communicate to adjacent and subordinate units and maneuver their forces in the area of operations (AO).

The current requirements by which units communicate with higher and coalition forces have meant that they must use different physical machines, each with a special network configuration. The result is a large logistical-support burden; and as supply convoys dispatch to subordinate units, service members

come under increased threat from the enemy. The Commandant of the Marine Corps (CMC) has tasked investments in C2, via the 2012 S&TSP. The focus is on three areas required to implement the MAGTF C2 plan: communications and networking systems to enable data exchange with and among distributed tactical forces; decision-support systems; and effective combat identification of enemy combatants, friendly forces, and non-combatants.

B. EMERGENCY OPERATIONS CENTER IN A BOX

Leveraging the original EOC-in-a-box platform (referred to as “EOC” hereafter), units can potentially increase communications while simultaneously reducing their footprint and power requirements, affording increased mobility without sacrificing capability. The EOC is a communications-command center that uses virtual-machines (VMs) to satisfy the vast majority of its network-communications requirements. It currently operates within the Monterey County government (Barreto, 2011) in Monterey California and provides the county with a small, lightweight virtual network to cover their network needs. It is available as a backup in case of a natural disaster to provide the county with a mirrored alternative to its current networking—in effect, an ad-hoc HFN ready to go when the county network fails due to unforeseen circumstances.

1. Hastily Formed Networks

HFNs (Denning, 2006) and virtualization are two distinct models that have been merged to form a system of systems (SoS) comprising power sources, communications, and a mobile EOC. The present EOC, as defined by Barreto (2011), and the HFN (Denning, 2006) have deployed with NPS faculty and Monterey-area fire-and-rescue agencies to such locations as New Orleans, Louisiana, and Haiti. They have provided ad-hoc networking for disaster-relief workers, emergency responders, and civilians. Technological capabilities include radio communications, Internet access, and Internet-protocol (IP) (Postel, 1981) telephones, to name a few. Barreto (2011) enabled the system to access

applications and data that users find important to their missions and cannot access with a web browser.

Denning (2006) defines an HFN as exhibiting five characteristics:

1. A network of people, established rapidly
2. From different communities
3. Working together in a shared conversation space
4. In which they plan, commit to, and execute actions
5. To fulfill a large, urgent mission

The shared conversation space created in the HFN model is the area that most stands to benefit from virtualization.

Virtualization is a technique that allows the abstraction of multiple computers and applications from a single computer or application. Under virtualization, all the advances in hardware and software technologies can be made to converge and operate seamlessly. Introducing virtualization technologies into the HFN architecture yields a robust EOC with virtualized servers, desktops, and applications augmenting existing HFN power and communications systems.

This research examines the degree to which the communications gap identified in the USMC S&TSP can be bridged using EOC concepts. A study of the compatibility of the EOC and current USMC software has not previously been undertaken. If compatible, EOC concepts can be expected to further the goal of expanding battlefield communications while easing the logistical burdens associated with a COC. It may also be possible to employ this system in smaller units in distant and austere environments, consistent with the USMC strategic plan of enhancing company and MAGTF operations while maintaining expeditionary maneuver warfare capabilities (USMC, 2012). The problems the researcher seeks to address are in the following realms:

2. Virtual Machines and Architecture

Virtualization is the process of building simulations, or virtual versions, of infrastructure resources such as computer environments, Operating Systems, storage devices, and network components, as opposed to supplying actual, or physical, versions of these resources. Thus virtualization results in a lower cost and size for a given network. Virtual-machine (VM) computers are commonly associated with standalone or client-side computers, where they operate with an Operating System (OS) or Internet browser (Venkatesh, Otis, & Bretl, 2001). Virtualization has become an important tool in computer design, and VMs are used in a number of sub-disciplines, ranging from OSs to processor architectures (Smith & Nair, 2005). Virtualization is not a new technology; rather, it is old technology repackaged, dating back to the 1990s, when it was primarily used to re-create end-user environments on a single mainframe to save on costs while testing new software (Ray & Schultz, 2009). There are three basic categories of virtualization, distinguished primarily by computing architecture:

- **Storage** Combines multiple networked storage devices so they can appear as a single storage device.
- **Network** Combines computing resources by splitting the available bandwidth into independent channels and assigning them to a server or device to operate in real-time
- **Server** Hides the physical nature of server resources and provides a virtual version with all server resources incorporated. This includes hiding the number and identity of individual servers, processors, and OSs from the software running them.

Server virtualization, the most common kind, is the primary driver of this technology and what most people mean by “virtualization” (Ray & Schultz, 2009).

VMs can operate in conjunction with or on a server computer that serves one or more client computers. These clients may be connected to the server directly (whether hard lined or wirelessly) or by networked connections. Enhancing software interoperability, system impregnability, and platform versatility (Smith & Nair, 2005), virtualization is the key technology underlying

cloud computing, which is quickly becoming the platform of choice for many companies (Szefer, Keller, Lee & Rexford, 2011). Understanding the architecture of a VM network is a paramount concern, due to the security risks associated with this technology.

Virtual environments rely on a hypervisor, or virtual-machines monitor (VMM), a software layer that lies between the VM and the physical hardware and manages how hardware platforms are shared among multiple guest OSs (Azab et al., 2010). Simply put, it provides a logical, rather than physical, view of computing resources. A guest OS, according to the U.S. National Institute of Standards and Technology (NIST) special publication (SP) 800-125, is an OS that is installed on a VM or disk partition in addition to the host, or main OS. The guest OS is managed by the VMM, which controls the flow of instructions between the guest OS and physical hardware (Scarfone, Souppaya & Hoffman, 2011). The VMM allocates resources such as main memory and peripherals to the VM. It gives each VM the illusion of being run on its own hardware by exposing a set of virtual-hardware devices (e.g., CPU, memory, NIC, storage), whose tasks are then scheduled on the actual physical hardware (Perez-Botero, Szefer & Lee, 2013). This allows a VM to circumvent real-machine compatibility and hardware-resource constraints and presents the guest VM with the illusion that the OS and applications inside the VM are running directly on some given software. There are two variations of the VM architecture: hosted and bare metal. Figure 1 depicts these variations.

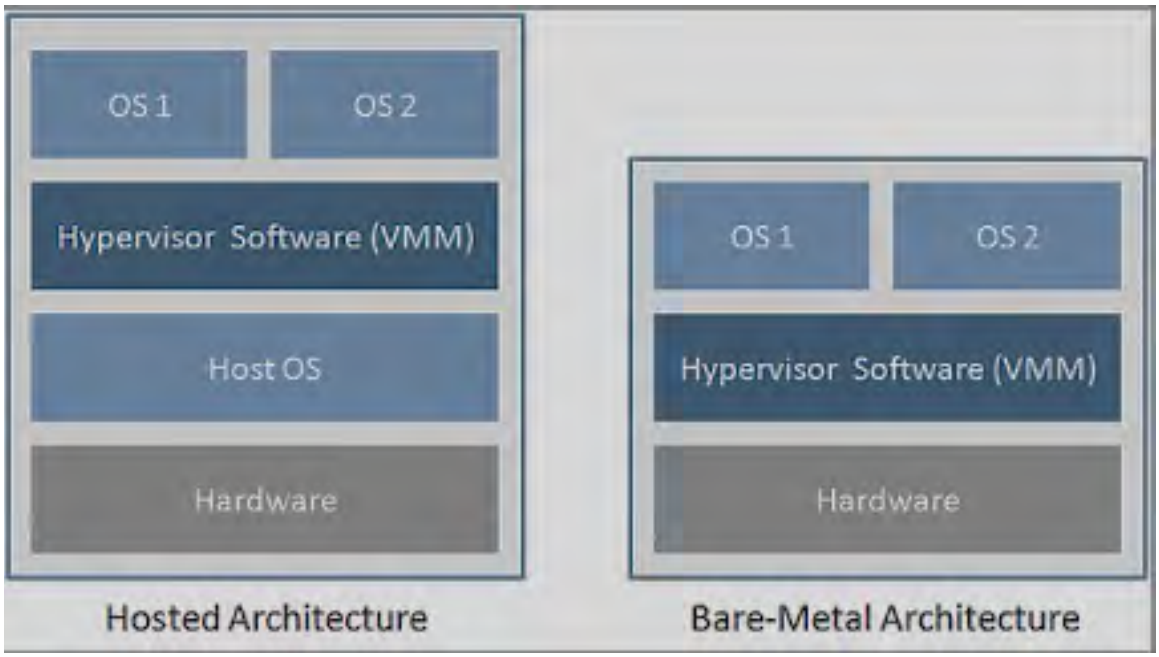

Figure 1. The architecture on the left depicts the VMM software installed on the host OS. The architecture on the right depicts the VMM software installed on the hardware and the OS installed on the hypervisor (from NIST SP 800-125, 2011).

a. Hosted and Bare-Metal Architecture

NIST SP 800-125 (2011) provides a description of hosted and bare-metal virtualization (also known as native virtualization). Hosted virtualization runs on top of the host OS, which can be almost any common OS (e.g., Windows, Linux, Macintosh). Hosted virtualization usually has an additional layer of software present running in the guest OS to provide utilities for controlling the virtualization from the guest OS, including file sharing, running web browsers, and emailing clients alongside the hosted virtualization application. Bare-metal architecture does not possess this capability; it can only run applications within the virtual system (Scarfone et al., 2011). In this architecture, the VMM runs directly on the underlying hardware, without a host OS. This architecture is often used to virtualize servers, just as hosted architecture is often used to virtualize desktops. Choosing which architecture to employ is an important decision for both operational and security reasons, as discussed in Section 5.

3. Virtualization of the COC Using the EOC Concept

Virtualization of the current COC presents manifold opportunities to meet USMC communications goals. Some advantages are server consolidation, lower energy consumption, faster hardware, expanded networking, maximal efficiency (Oh, Lim, Choi, & Ryoo, 2011), ease of adding programs, common access to multiple OSs and networks, and increased capabilities. With the potential of reducing the physical size of a COC, virtualization raises the prospect of providing small combat elements, such as platoons or squads, with functionality equal to battalion or regimental COCs—without the hardware requirements and accompanying logistical burdens.

Providing potential benefits beyond the USMC's communication goals, the EOC is a model for conceiving, structuring, synthesizing, and delivering sophisticated, tailor-made communications in hours or days, rather than months or years. The EOC concept revolves around user-centric, on-demand communications. This makes the EOC extremely flexible with various software and communication needs and enables the system to adapt to the user, as opposed to the user's adapting to the system.

In addition, with the use of VMs, the EOC can facilitate seamless information sharing down to the platform level and enable the integration of unclassified and classified systems for joint and coalition operations, in line with the USMC's strategic plan of 2012. This could enhance the commander's ability to pull information from higher or outside sources and save on data storage by tapping into the Internet or a cloud.

4. Cloud Computing (Portable, Private Clouds)

Cloud computing is not a single, unitary thing. There is no "the cloud", or a clear difference between the cloud and the Internet itself (Ryan, Falvey & Merchant, 2013). The concept of cloud computing dates back to 1953, with Herbert Grosch's theory that computing performance would increase by the square of its cost and that relatively dumb terminals would tap into the power of

large data centers (Gorsch, 1953). Since the early 1990s, there has been an effort to legally define the meaning of “cloud computing”. The term originated with Compaq marketing executive George Favaloro in 1996 (Ryan et al., 2013), who described a trend toward more intra- and intercompany connectivity, e-commerce, and use of the Internet as an information source (Regalado, 2011).

While there is no official definition, computing researchers and practitioners have defined “cloud” in various ways. Buyya, Yeo, and Venugopal (2008), assert that a cloud is a type of parallel, distributed system consisting of a collection of interconnected and virtualized computers, dynamically provisioned and presented as one or more unified computing resource, based on service-level agreements established through negotiation between a service provider and customer.

With the rising popularity and evolving paradigm of cloud computing, the NIST in 2011 defined “cloud computing” as

> A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, application and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction. (Mell & Grance, 2011, p. 2)

NIST SP 800-145 organized the cloud model according to five essential characteristics (on-demand, self-service; broad network access; resource pooling; rapid elasticity; and measured service), three service models (software, platform, and infrastructure), and four cloud-deployment models (private, community, public, and hybrid) (Mell & Grance, 2011). However, other organizations outside of the U.S. offer competing definitions. For this thesis, we use the definition established by NIST (2011).

Cloud-computing services offer the ability to scale computing requirements up or down and reduce the cost of deployment. Many organizations are migrating to cloud computing services to lower risk, reduce information technology (IT) costs, and provide better business continuity (Mandal & Khilar,

2013). Cloud computing frees customers of the expense and hassle of installing and maintaining applications locally, lowers the cost of application development, and makes the process more scalable (Leavitt, 2009) and flexible.

The Department of Defense (DOD) and federal government have also adopted cloud computing in an effort to reduce IT costs. The federal government spends billions of dollars annually on IT infrastructure and is shifting to cloud computing to maximize the use of those funds under the president's budget (U.S. Government Accountability Office, 2010). Since cloud computing is managed by an external provider and relies on Internet-based services and resources, it frees the customer from the expense of maintaining IT networks (U.S. Government Accountability Office 2010). As the government looks toward cloud computing within its garrison IT infrastructure, it envisions cloud computing for the DOD and troops in combat, to allow access on demand, regardless of time and location. This concept conforms to the DOD Chief Information Officer's (CIO's) responsibility to address international issues associated with IT and communications technologies for the non-automatic movement, transmission, and reception of information (Department of Defense, 2005).

As the DOD CIO states, "Long term planning is essential, but at the same time we have to be focused on the individuals on the ground and providing them with what they need" (Corrin, 2011, para. 6). One benefit that cloud computing offers the DOD is battle-space situational awareness with the common operating picture (Kubic, 2008). Accessing the cloud and being able to view the status of troops, missions, weapons, and supplies, as well as tactical intelligence, surveillance, and reconnaissance (ISR) feeds from anywhere in the world, can give the strategic and tactical warfighter the resources necessary to prevail (Kubic, 2008).

DOD missions can be unpredictable and range from large-scale strategic operations to small-scale conflicts in austere environments. With the increased reliance on small units and SOF, there is a need for lightweight mobile communications assets that are flexible and scalable to the situation and

mission. By providing a portable private cloud (PPC), the EOC could improve operational and tactical effectiveness for forward-deployed forces by mirroring the capabilities of the current COC in a smaller configuration, improving small-unit maneuverability and enhancing communications capabilities.

5. Virtualization Security Challenges

Many organizations are gravitating to virtualization, with estimates showing between 60 and 80 percent of IT departments pursing server consolidation (Ray & Schultz, 2009) as a way to significantly reduce costs. Yet these organizations may be overlooking the security drawbacks associated with operating multiple machines on the same physical hardware. Consumers need to understand that migrating to a virtual environment does not reduce vulnerabilities and threats. If a service with inherent vulnerabilities is moved from a non-virtualized server to a virtualized server, it remains vulnerable to exploitation, according to NIST SP 800-125.

While in principle, migrating to a virtual environment will produce some benefits, it also adds vulnerabilities and threats. These threats and vulnerabilities include exploitable weaknesses in virtualization software, the existence of covert channels, and the possibility of new types of malware (van Cleeff, Pieters, & Wieringa, 2009), as well as hyperjacking and virtual-machine jumping. These weaknesses can prove costly in the event of an attack. Identifying vulnerabilities and protecting the triad of infrastructure confidentiality, integrity, and availability (CIA) is especially vital in the DOD.

Many of the features of virtualization offer both benefits and disadvantages in the realm of security (Scarfone et al., 2011). As a whole, virtualization improves availability, but threatens confidentiality and integrity, even though many features are designed with these goals in mind. A number of threats to virtualization have been recognized and addressed and some can be mitigated. As asserted by Ray and Schultz (2004), VMs can be used to isolate processes from attackers and malware, making systems and applications more

difficult to attack or infect. Secure isolation, that is, confining a program to a virtual environment, is a basic concept in virtualization, and should guarantee that any action performed inside the VM cannot interfere with the system that hosts it (Ray & Schultz, 2004). Once again, the physical host server must have a proper security protocol in place; if compromised, all the VMs and applications on the host server will be affected.

Since the security of a virtual network depends on the individual security of each component, organizations should secure all these elements. With the assumption that the physical host OS, guest OS, applications, and storage have proper security protocols implemented, this research focuses on the critical vulnerability of virtualization: an attack on the VMM.

The programs that control the VMM should be secured using methods similar to those used for other software on desktops and servers, according to NIST SP 800-125. Scarfone et al., (2011) agree that the critical vulnerability of the virtual infrastructure depends on the security of the virtualization management system (VMS) that controls the VMM and allows the operator to start guest OSs, create new guest OS images, and perform other actions. Due to security implications, access to the VMS must be restricted to authorize personnel only. Securing each VMM interface and limiting access to the VMM is critical to the security of the entire system (Scarfone et al., 2011).

An attack on the virtualization infrastructure via the VMM can cause serious damage to a VM, because the VMM has more access to hardware resources than typical applications do. Two primary attacks are explored in this thesis: hyperjacking and virtual-machine jumping.

a. Hyperjacking

By creating and inserting a thin hypervisor into the virtualization system, an attacker can take control of the underlying OS. Traditional security measures are ineffective against this threat, because the OS, which runs above the VMM, is not aware that the machine has been attacked.

b. Virtual-Machine Jumping

Virtual-machine jumping exploits vulnerabilities in the VMM that enable malware or a remote attacker to compromise VM protections and gain access to other VMs, or even the VMM itself.

These attacks are often conducted once an attacker has gained access to a weakly secured virtual-machine. An example of hyperjacking is a software called Blue Pill Rootkit (Perez & van Doorn, 2008), developed by Joanna Rutkowska, which evades all detection from system administrators and allows its toolkit to take control of the OS (Oh et al., 2011). Since the hypervisor has frequent interaction with the guest VM, a malicious VM can use it to hyperjack the hypervisor or implement a virtual-machine jump. Either attack can give the attacker access to the hypervisor. Once the attacker has access, he can access all VMs attached to the hypervisor without detection. From there, the attacker can exploit the virtualization software, gaining the ability to obstruct or access other VMs and thus breaching the CIA triad (Szefer et al., 2011).

6. Software Compatibility

EOC components and current virtual capabilities allow software to be stored on the device, which allows users to operate with the system. However, the EOC system has not been tested for compatibility with current and possible USMC Tactical Data Systems (TDS), listed in Appendix A, or the COC tactical software also known as Joint Tactical Common Workstation (JTCW), listed in Appendix E.

7. Energy Requirements/Reduction Possibilities

In the past 10 years, the USMC's consumption of energy on the battlefield has increased exponentially, driven by new and powerful war-fighting capabilities that have made the USMC dependent on logistical trains, which are exposed to risks. Currently, the Medium Tactical Vehicle Replacement (MTVR), which is the workhorse of the USMC logistical trains, consumes 50 percent of all fuels used

by USMC vehicles on the battlefield (Goodman, 2010). Combine this with the fact that power consumption in information and communication technology is ten percent of the total energy consumed in industrial countries (Ghaziseedi, Wang & Tafazolli, 2012), tends to lend additional fuel requirements on the USMC. The USMC has realized this and is focusing efforts toward reducing fuel consumption, as stated in the USMC S&TSP (2012). The CMC has described the Corps' energy priorities with the following statement:

> The current and future operating environment requires an expeditionary mindset geared towards increased efficiency and reduced consumption, which will make out forces lighter and faster. We will aggressively pursue innovative solutions to reduce energy demand in our platforms and systems, to increase out self-sufficiency in our sustainment and reduce our expeditionary footprint on the battlefield. Transforming the way we use energy is essential to rebalance our Corps and prepare it for the future. (35th Commandant's Planning Guidance, 2010, p. 3)

The USMC Expeditionary Energy Strategy (2012) is aimed at increasing energy performance, efficiency, and self-sufficiency and reducing logistical vulnerabilities, to yield a lighter, more maneuverable, enhanced MAGTF operations-capable force (2012 USMC S&TSP).

8. Mobility

Provision of "on the move" (OTM) capabilities has become essential in tactical networks as the paradigm shifts to network-centric warfare (NCW). The need for maintaining expeditionary requirements without sacrificing capability is highlighted in the USMC S&TSP (2012). The intent is to improve mobility for the entire MAGTF while reducing logistical footprints and fuel consumption. The USMC Installation and Logistics Roadmap (2013) characterizes expeditionary logistics as:

- Lighter, modular, more energy efficient
- Responsive, reliable, scalable, and timely
- Supporting MAGTF fires, maneuvers, and force protection

- Leveraging technology to improve logistical capabilities, capacity, and interoperability
- Providing MAGTF C2 capability to deployment and distribution operations
- Creating an information network that transmits information and services via assured end-to-end connectivity

The EOC can potentially satisfy this vision while at the same time providing a PPC, with the potential to improve operational, logistical, and tactical communications for forward-deployed forces by mirroring COCs in a smaller configuration. This sizing down theoretically allows a platoon or smaller SOF unit, operating in a stationary position for a brief or prolonged period, to employ an EOC with little effect on maneuverability—contrasting dramatically with the hampering effects of a hardware-reliant COC. The unit would be able to relocate quickly and save fuel while still enjoying full communications. However, in judging the EOC as a plausible option, overall weight is a significant consideration.

Since lift and lift-and-carry (L-L&C) are the most frequently performed physically demanding tasks in the military (Sharp, Rosenberger & Knapik, 2009), careful consideration must be taken in redesigning the existing EOC as not to add more weight for the members of a small or SOF unit to deal with. U.S. Military Standard 1472 F (1989) gives 79kg/174-lbs as the recommended limit for a two-man team lifting from floor level to 91cm/35.8-in. The standard recommends doubling the one-man load (39.5kg/87-lbs.) for a two-man L-L&C. While this standard is rarely followed when developing new gear, due to time restraints and the need to deploy the gear rapidly, it is adopted in this study.

In austere environments, the USMC deploys small units forward of its main battalions (BNs) or headquarters (HQs) to establish and maintain FOBs or combat outpost (COP) positions for defensive and offensive tasks. These locations usually have little communications capability—in most cases, only an Army/Navy 117F multiband man-pack portable radio (AN/PRC) that operates on the very high-frequency (VHF) range. These radio systems provide half-duplex

voice communication and limited text messaging to the BN or HQ. Some elements may also be provided with a broadband global-area network (BGAN).

a. Broadband Global-Area Network

The BGAN system is a small satellite terminal and a laptop computer, as shown in Figure 2. The BGAN system allows the unit to access a satellite connection and provides limited data capabilities to communicate and share information with higher and adjacent units. The BGAN is limited to the capability of the laptop and the terminal data rate, which is normally 432 kpbs (Inmarsat, 2013). Owing to the cost and limited number of satellite channels, not all units are provided with this capability, and those who have it are limited by capabilities of the device used as a medium (the laptop). Moreover, the laptop can communicate outside the COP or FOB only, and does not allow communication within. This can create a bottleneck of information sharing among the units involved. Allowing internal sharing of information would be expected to improve efficiency and provide HQ with near-real-time information.

Figure 2. Small, Class-2 BGAN terminal for SATCOM-on-the-quick-halt (SOQH) at the dismount level, or fixed-site applications with Toughbook (from Inmarsat, 2013).

C. THE EOC

The EOC is built as a mobile device for local and state emergency-service organizations, providing a portable network with wireless capabilities to facilitate internal and external information sharing. In its current configuration, the EOC is not compatible with austere conditions and would require redesign to meet USMC size, weight, and power consumption requirements.

EOC Characteristics

The EOC as designed consists of eight COTS components (Barreto, 2011):

1. **A virtual-desktop infrastructure (VDI)** This is the core component that provides the EOC with 100 solid-state-disk (SSD) drives, 2x1 gigabits-per-second (Gbps) copper and 2x10 Gbps fiber-network adapters, supporting up to 100 virtual desktops.

2. **A hard disk drive (HDD)** provides additional storage of up to twelve terabytes (TBs).

3. **A CISCO SGE200P switch** provides internal communications among devices via 24 ports.

4. **A wireless router** This is a Cisco WRT 400N wireless router/access point that provides internal network service, an IEEE 802.11n wireless hotspot, and support for two RF radios simultaneously.

5. **A keyboard, video monitor, and mouse (KVM)** manages the VMware system, with a slide-out keyboard and a 19" LCD display.

6. **An uninterruptible power supply (UPS)** provides a stable backup-power source to prevent sudden power loss and surges.

7. **A power-distribution unit** (PDU) provides additional 120volt power outlets.

8. **A rack chassis** houses the components.

The current EOC weighs approximately 244 pounds and meets the criteria of robustness, energy efficiency, two-man portability and integration with HFN systems (Barreto, 2011). These criteria fit with USMC deployable systems;

however, the EOC is too heavy for small-unit mobility. This research suggests that the EOC configuration can be modified to reduce weight to within 174 pounds, compliant with the U.S. Military Standard 1472F (1989) for a two-man L-L&C, which would make it a viable option for small units at the tactical edge.

a. EOC Overview

The EOC as described and field tested by Barreto (2011) can meet power requirements identified by the CMC. The measured power consumption for the EOC was calculated at 550.04 watts per hour (W/h) of power. Figure 3 depicts the power consumption of the EOC server, switch, KVM, and SAN, as tested by Barreto (2011).

Equipment	Qty	Power (Watts)	Power Total (Watts)	Current (Amps)	Current Total (Amps)
V3 STRATO 100 Server	1	Left P/S 100.15 Right P/S 91.82	191.97	Left P/S 0.88 Right P/S 0.82	1.7
Cisco SGE2000P Switch	1	20.27	20.27	0.19	0.19
TRIPP-LITE B021-000-19 KVM	1	<1	1	<1	1
Coraid SRX3500 SAN	1	336.8	336.8	2.8	2.8
		System Total	550.04		5.69

Figure 3. EOC Component Power Consumption (from Barreto, 2011).

As tested by Barreto (2011) the EOC can function under its current configuration with a minimal amount of fuel. This research suggests that additional modifications could further reduce power requirements, making the EOC compatible with USMC alternative fuel technologies currently under testing.

The demand for additional C2 has increased fuel consumption and the supply logistics needed. Historically, vehicle electronics systems had a relatively low duty cycle (the period in which the electronics draw power from the vehicle, relative to the period when they do not). In other words, vehicles were not required to be on or powered for very long periods. For example, a vehicle's electrical system (or, for some stationary vehicles, external generators) was used

to power vehicle-mounted radios. The radios could be monitored for short periods while the engine was off, but the vehicle or generator would have to be running to support the radios for longer periods or when the radio was transmitting regularly. Today, however, the duty cycle to support the growing amount of electronics, sensors, jammers, and communications equipment for most military vehicles is fast approaching 100 percent. Engines need to keep running almost continuously to power electronic equipment, burning a great deal of fuel (Kelly et al., 2011). The need to reduce fuel consumption without degrading communications is critical to reducing the costs and casualties associated with refueling during combat.

III. CURRENT MARINE CORPS C2 TECHNOLOGY

A. BACKGROUND

According to USMC Doctrinal Publication (MCDP) 6, no activity in war is more important than C2. C2 by itself will not guarantee success in a single attack against an enemy force or destroy a single enemy target. It will not affect a single emergency resupply. Yet none of these essential war-fighting activities, or any others, would be possible without effective C2. Without C2, campaigns, battles, and organized engagements are impossible, military units degenerate into mobs, and the subordination of military force to policy is replaced by random violence. C2 is grounded in the tenets of Marine Corps maneuver doctrine and has been enforced for generations. When combat operations in Iraq and Afghanistan pushed the limits of the Marine Corps' C2 capabilities, commanders began to request assets to close the emerging gaps while engaging the enemy rapidly in austere environments. These requests were communicated via universal-needs statements (UNS).

An UNS identifies mission-critical capability gaps and deficiencies (USMC, 2008). The request is initiated by a combatant-command-level Marine component commander, who identifies a war-fighting capability that is critically needed by forces conducting combat or contingency operations. Failure to deliver on the request is likely to prevent units from accomplishing their mission and increases the probability of casualty and fatality (MCO 3900.17, 2008).

This chapter examines combatant-commander (COCOM) requests, made during combat operations, to fill the C2 gap. It also discusses current and emerging C2 capabilities and infrastructures aimed at closing the C2 gap, and explores the concept of pushing communications capabilities to platoon, squad and small SOF elements via technology pioneered at NPS and used by first responders. This background allows us to consider some real-world applications of C2 technology in situations similar to what USMC forces may experience.

B. EXPEDITIONARY CONSIDERATIONS

With the application of modern virtualization technology to the C2 realm, the first-responder community (FRC), with the assistance of the Naval Postgraduate School, has implemented a C2 structure using COTS technology—overcoming inherent limitations to achieve unprecedented coverage, throughput, and flexibility in environments with limited or no communications infrastructure. This work, leveraging the EOC concept developed by Barreto (2011), offers a new model of seamless mobility that has transformed data and voice communications for civilian and police responders in natural disasters and other settings where instant wireless access offers quality of life and safety benefits. Operating in austere environments with limited or no communication infrastructure, the FRC has used COTS systems to offer C2 capabilities to decision makers, allowing them to coordinate relief efforts. This technology could potentially prove applicable to expeditious requirements at the tactical edge, and recent work within the FRC could assist USMC efforts in C2 infrastructure and capability development.

To understand why COTS technology is of interest in meeting COCOM capability requests, it is necessary to understand that C2 capabilities are critical to the USMC for doctrinal reasons. Units must have mobility, swift exchange of orders, and fast-flowing information that allows the commander to shape the battle space. Commanders must be able to recognize what needs to be done and take appropriate, decisive, harmonious, and secure action that raises situational awareness (USMC, 2013). All this is encompassed in the MAGTF's version of C2 requirements.

1. MAGTF C2 Systems Characteristics

The USMC Systems Command (MARCORSYSCOM) cites the following characteristics of USMC C2 technology:

- **Common** Command echelons use the same equipment. Unique MAGTF sensors and intelligence feeds enter via a standard gateway.

- **Modular** C2 and communications system are designed to enable component utilization that logically supports a variety of configurations for various C2 echelons across the MAGTF.

- **Scalable** Software and hardware components are added and subtracted to facilitate C2 functions for all MAGTF operations centers.

- **Interoperable** C2 and communications systems must have the interoperability necessary to ensure success in joint and multinational operations, as well as interactions with other government agencies (OGAs) and non-governmental organizations (NGOs).

- **Agile** To support expeditionary forces and operational concepts, a communications system must be agile. The key dimensions of C2 and communications system agility are:

    - **Responsive** The ability to react in a timely manner to a change in the environment.
    - **Flexible** Able to employ multiple methods to succeed and the capacity to move seamlessly between them.
    - **Innovative** Able to do old things in a new way or simply try new things.
    - **Adaptable** Able to change the organization and work processes.
    - **Reliable** Available when needed and perform as intended with low failure rates and few errors.

- **Trusted** C2 and communications system users must have confidence in the capabilities of the network and the validity of the information made available by the network.

- **Shared** Sharing allows the mutual use of the information services or capabilities among entities of the operational environment. This ability may cross-functional or organizational boundaries (MARCORSYSCOM, 2012).

With these characteristics identified, the USMC has focused on providing the COCOM with communication assets to complement maneuver doctrine and information sharing. With today's technological advances, it is possible and advantageous to leverage military technology with COTS technology to enhance

the COCOM's ability to maneuver throughout the AO while maintaining the MAGTF's C2 requirements.

> The Marine Corps recognizes the trend in evolving information needs with in garrison and tactical environments and the need to provide an agile method of meeting those needs. (Director for Command, Control, Communications, and Computers (C4) and the Department of the Navy Deputy Chief Information Officer, 2013, p. 3)

This strategy emphasizes a focus on the user and the ability to share information. Raised situational awareness from information sharing, both in garrison and deployed roles, will enable more efficient mission execution (Director for Command, Control, Communications, & Computers (C4) and the Department of the Navy Deputy Chief Information Officer, 2013).

Historically, these capabilities satisfied the need for COCOMs and small-unit leaders who relied primarily upon voice radios, with minimal data capability, to receive the commander's intent and execute missions. While this method of voice transmission was adequate in the past, the complexity of the environment has changed. As our enemies have become increasingly unconventional and attack using asymmetric methods, our small-unit leaders are increasingly relied upon to counter them, and they must have better situational awareness (SA), bandwidth and network services to do so. In essence, they must be smarter and better informed than the enemy. With units dispersed throughout the battlefield, there is a need for flexibility and ubiquitous information-sharing to raise SA and speed up decision making and mission accomplishment (Director for C4 and the Department of the Navy Deputy Chief Information Officer, 2013). All elements operating away from their main COC should be able to exploit the rapidly changing dynamic in the field and participate in the rapid dissemination of information to high, adjacent, and supporting units. Gone are the days of FOB-centric architecture; the trend is toward a more robust, warfighter-centric model. Forward-operating, small-unit Marines require a robust voice and data

communication capability. The USMC communications arsenal is lacking in this area.

1. Current Marine Corps Communications Assets

In keeping with doctrine and evolving battlefield dynamics, the USMC seeks a deployable, mobile, flexible, self-contained facility that lets units scale up or down their communications equipment depending on the mission, unit size, and ability to maintain the tenets of the MAGTF. To achieve this, the USMC has looked to both military and civilian industry to develop a system of systems that promotes the war-fighting functions (intelligence, maneuver, fires, C2, logistics, and force protection) (Director for C4 and the Department of the Navy Deputy Chief Information Officer, 2013, p. 3). Many projects are underway to satisfy these requirements.

a. Combat-Operations-Center Capabilities Set

In 2002, General Dynamics Decision Systems developed the COC-capability set (CAPSET), by which the COC was designed as the focal point of decision making during all phases of ground warfare. This strategy allows Marine forces to centralize C2 and digitally collect, process, and disseminate tactical data to subordinate, higher and adjacent elements. The COC CAPSET contains four variations to accommodate different command levels (e.g., regiment, battalion, company) allowing a deployable, self-contained, centralized facility that permits scaling, depending on requirements. Figure 4 illustrates the various COCs.

Variant	Unit Size
AN/TSQ-239(V)1	*MEF*
AN/TSQ-239(V)2	MEB
AN/TSQ-239(V)3	Regt/Group
AN/TSQ-239(V)4	Bn/Sqd

Figure 4. EOC COC CAPSET Configurations (from Headquarters USMC, Combat Development and Integration, 2011).

All CAPSETs are designed using COTS, to be a mobile, modular C2 center able to support Marines wherever they deployed. The integrated package hosts current mission application software, interfaces to USMC communications assets, and leverages organic table-of-equipment (T/E) vehicles for transport to the field (Headquarters USMC, Combat Development and Integration, 2011). This system provides a low-risk operation center that could:

- Increase operational capability and mission effectiveness
- Speed decision making
- Enhance situational awareness

MAGTF C2 CAPSETs are a logical grouping of services or capabilities that support the organizational structure of the MAGTF and are equipped with a

minimal standard basic package, which includes the items shown in figures 4 and 5.

The differences between CAPSETs are based on equipment quantity and TDS capabilities (Appendix A). The size of a Marine unit dictates the size of the CAPSET they operate. CAPSET IV, which is the smallest of the CAPSETs, is tailored for elements at the level of BNs, Marine Air Groups (MAGs), and Marine Wing Support Squadrons (MWSS) (Lawlor, 2004). The USMC Technical Manual (TM) 2000-OD/2C (2005) provides the following description of the major components and characteristics for the COC CAPSETs IV (see also figures 5 and 6) and Appendix D provides a list of the CAPSET IV's IT equipment:

b. COC Major Components and Characteristics

CAPSET IV COC displacement relies on two vehicles maintained by the owning units. The vehicles are the model (M) 1152 High Mobility, Multipurpose Wheeled Vehicle (HMMWV) A2s, which is used as the prime movers. They can facilitate the connection of up to 24 external radios, using two digital switching units (DSU); antennas can be located up to 2 km away, using fiber-optic cable.

Transport	Truck, rail, ship, aircraft or helicopter		
Power Requirements	120/208 VAC, 60 Hz, 3-phase		
Size and Weight		Operational Trailer	Supplemental Equipment
	(GETT)	(OT)	(SEIII)
Weight	4,165 lb.	4,196 lb.	3,620 lb.
Weight (Tongue)	348 lb.	376 lb.	N/A
Length	160 in.	132 in.	N/A
Width	86 in.	86 in.	N/A
Height	72 in.	86 in.	N/A
Square	95.6 sq. ft.	78.8 sq. ft.	N/A
Cube	573.4 cu. ft.	565 cu. ft.	331 cu. ft.

NOTE

"SE" denotes "supplemental equipment": components not transported on either the OT or GETT, but are transported in the HMMWV, or other vehicle, at unit discretion.

Figure 5. COC CAPSET IV Technical Characteristics, according to TM 2000-OD/2C (from USMC TM2000-OD/2C, 2005).

Qty	Item	Qty	Item
1	20 kW COTS Generator, 96K BTU COTS Environmental Control Unit, and COTS "quick-erect" Tent integrated on a modified M1102 Trailer (GETT)	1	MEP531A 2 kW
		1	Interactive Whiteboard
		1	COTS Medium Format Printer
		1	Large Screen Display System
1	Electronics Equipment and Peripherals Suite for COC Functionality (OT)	2	Digital Switching Unit (DSU)
		3	Uninterruptible Power Supply (UPS)
8	Notebook PC/workstations	4	Crypto Device, KIV-7
1	SIPR/NIPR LAN	1	Intercom System

Figure 6. COC CAPSET IV Major Components according to TM 2000-OD/2C (from USMC TM 2000-OD/2C, 2005).

The COC is advertised as having transportable C2 capability; however, the description should not be interpreted as indicating mobile C2 capabilities. This system was designed for ATH C2 and requires a fairly large footprint. It is cumbersome to move and logistically burdensome in the expeditionary environment, as suggested by the amount of equipment that constitutes the CAPSET (see Appendix B for a complete gear list). The term "transportable C2" in the context of the COC implies that the COC system is self-contained, can be deployed or displaced to various locations, and, depending on the CAPSET, can be erected and operational in six to eight hours (Headquarters USMC, Combat Development and Integration, 2011).

c. COC Mobile Capability

The COC can provide the commander with tactical or "jump" capability. A jump COC allows the commander and staff to be physically removed from the main COC while maintaining some of the same capabilities. This allows the commander to insert himself at the point of friction to provide effective C2. The use of wheeled or tracked vehicles is typically required to ensure the commander can move and communicate simultaneously. This mobility also enables the jump COC to assume C2 responsibilities, allowing the main COC to be packed up and moved (Liguori & Daniel, 2013). The COC was not designed to provide the jump with mirrored main-COC communication architecture or for distribution to units smaller than a BN, MAG, or MWSS.

The COC is a SoS that integrates and interfaces to an array of systems and equipment that can be organized according to the MAGTF C2 capability model.

d. Tactical Data Systems

According to Headquarters USMC, Combat Development and Integration (2011), the COC hosts TDS and applications and the JTCW software, providing the commander with tools to maintain SA, plan, make decisions, direct units, and monitor execution, enabling the integration of systems (see system relationships in Appendix A). The COC itself does not manage the TDS or application data, as shown in Appendix A; it simply provides hosting, storage, a user interface, and a display.

However, the COC program does provide a core set of service capabilities to hosted applications and TDSs; these include the enterprise services that allow the COC to provide access and deliver information to the global information grid (GIG). The COC does not directly connect to the GIG or provide services across the USMC enterprise, and the COC is dependent on the availability and capability of the transmission system (Headquarters USMC, Combat Development and Integration, 2011).

2. The Networking-on-the-Move (NOTM) System

With continuous military operations in austere environments and the need to extend C2 beyond VHF range, commanders require the ability to rapidly engage the enemy while OTM. This means leveraging the C2 capabilities provided by the COC. NOTM, which is a system combining a variety of COTS, was approved to meet the emergent need identified by COCOMs via an urgent UNS (classified) request.

The NOTM system is described as a transformational C2 capability for all elements of the MAGTF (USMC Concepts and Programs, 2013). It is a self-forming, self-healing, mobile, ad-hoc, tactical-communications network. This

means the NOTM system does not require a nearby established infrastructure to operate, and it can be decentralized, self-organizing, and set to automatically reconfigure without human intervention in the event of degraded or broken links between transceivers. This provides units with the ability to have uninterrupted C2 while en route to an AO—and once they arrive, C2 is instantaneous. Providing the warfighter with an integrated voice, video, and data enables real-time C2 with OTM, beyond-line-of-sight (BLOS), and over-the-horizon (OTH) communication (MARCORSYSCOM, 2012). These capabilities help the COCOM, or any small-unit leader, exercise C2 in a dynamic environment. Figure 7 depicts the MACORSYSCOM (2014)-advertised topography of the NOTM network.

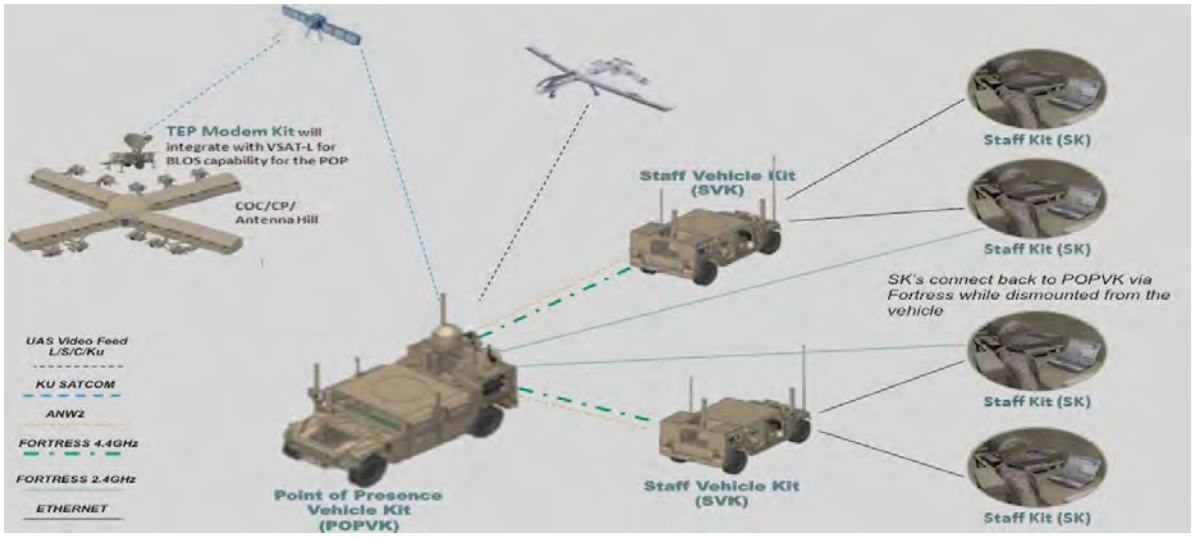

Figure 7. NOTM System Overview, Subsystem connectivity (from MARCORSYSCOM, 2014).

a. NOTM Provided Systems

According to MARCORSYSCOM (2014) the NOTM is a vehicle-based C2 system that provides COC capability to commanders and their staff while OTM or at-the-halt (ATH). This is achieved via an OTM SATCOM system and three external network enclaves (SIPRNET, NIPRNET, and mission specific). The NOTM system is predicted to provide the following systems to units:

- **A point of presence (POP)** A POP mounted on a host vehicle platform acts as the primary hub for mounted and dismounted users and bridges mobile users operating OTM to the network. POP provides SATCOM, LOS, and wireless radio-frequency, data-network, and communication-security (COMSEC) equipment within the host platform. The POP also hosts a video server, allowing direct video feeds.

- **Staff vehicle kits (SVKs)** Mounted on vehicles, SVKs provide users with extension nodes. The SVK hosts the mobile user's laptops and handheld devices and provides network connectivity and access to C2 applications through the POP to the ATH network. The SVK consists of LOS, wireless devices, and data-network equipment.

- **NOTM staff kits (SKs)** are for the dismounted user and provide an extension kit for LOS or wireless connectivity from laptop and handheld devices to the SVK or POP, via LOS or wireless technology.

The NOTM system suite currently consists of three tactical vehicles, with one equipped with the POP components and the other two equipped with the SVK components. This provides an extension of POP-Vs services, allowing for a further dispersion of C2. The system allows the extension of services to dismounted units by means of a communications man-pack component. Depicted in Figure 8, are the POP-V, SVK, SK, and tactical entry-point (TEP) modem-kit equipment set. The TEP modem is a stationary kit that provides the termination of the satellite downlink integrated with a support wide-area network (SWAN) version-3 terminal or a very small-aperture terminal–large (VSAT-L) at the COC's location (MARCORSYSCOM, 2014).

Figure 8. NOTM System Suite: HMMWV/M-ATV (from MARCORSYSCOM, 2014).

b. VSAT-L

The purpose of the SWAN-D/VSAT is to enable USMC intra-theater communications, allow forward-deployed elements to break the terrestrial line-of-sight tether (to extend their operations farther from their higher-echelon command), or to enable operations in terrain not conducive to line-of-sight (LOS) operations.

c. NOTM Major Components

To provide the COCOM with COC-like capabilities on the move, the NOTM is equipped with a variety of COTS technology. MARCORSYSCOM (2014) identifies the NOTM system and subsystem's major COTS components and their characteristics.

The point-of-presence vehicle consists of the following major components per asset and is considered the hub of this communication suite. The network topography of the POP-V is depicted in Figure 9. The POP-V kit consists of the following equipment:

- Ku-Band (12-18 KHz) SATCOM

- Video Scout
- AN/PRC-117G using adaptive networking wideband waveform- 2 (ANW).
- Fortress ES820 data radio (802.11a,b and g)
- DTECH ruggedized network models (bc router, switch, network enclaves)
- MPM-1000 (NCW) ruggedized modem:
- Tactical Operations Center Intercommunications (TOCNET) system Soft CAU Interface
- Antenna plane, antennas
- Shore power module connection
- Admin workstation with KVM

The staff vehicle kit consists of the following equipment per vehicle:

- AN/VRC-114 utilizing ANW2
- Fortress ES820 data radio (802.11a)
- Secure network (SECNET) 54 in-line encrypter
- Antenna plane

The staff kit consists of the following equipment per bag:

- Panasonic Toughbook CF-19
- Talon (KOV-26) card
- TOCNET soft CAU interface
- Ancillaries: webcam, cables
- Backpack with integrated docking station, power unit for dismounted use.

The **tactical entry-point modem kit** consists of the following:

- MPM–1000 (NCW) ruggedized modem
- CISCO 2901 BC router
- Network enclaves
- PACSTAR WAN accelerator
- Workstation CF-19 (Toughbook)

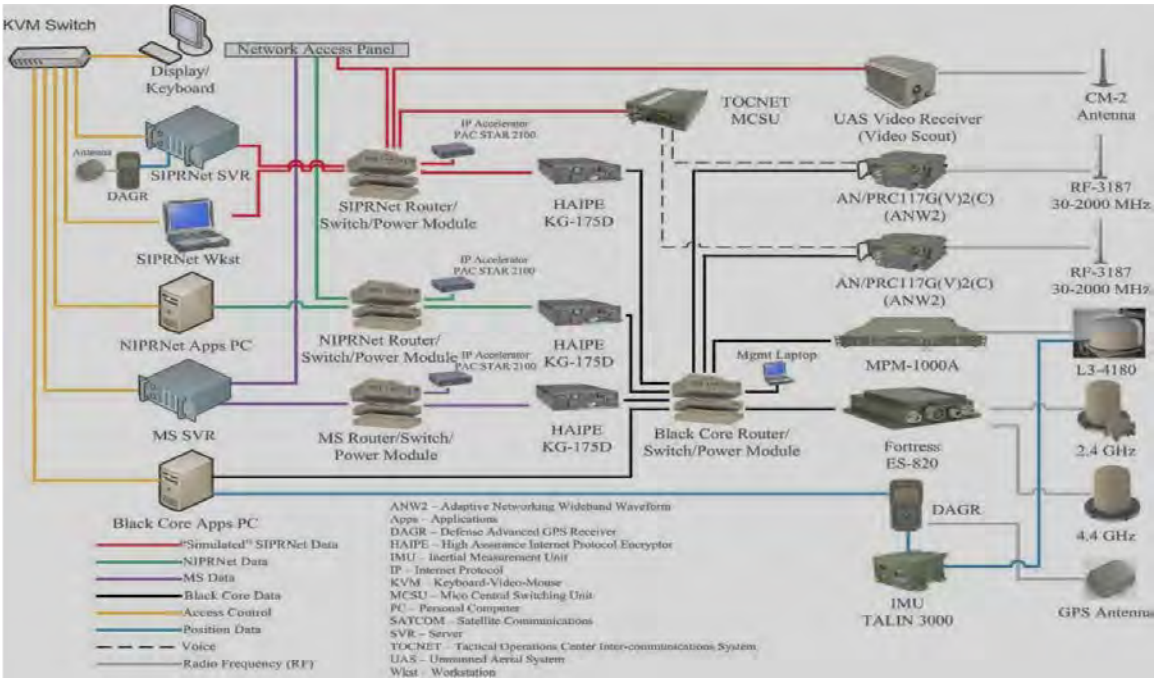

Figure 9. Point-of-Presence Vehicle Network (from MARCORSYSCOM, 2014).

d. Tactical Data Systems

According to MARCORSYSCOM (2014), the NOTM's POP-V and SKs host the JTCW software. The JTCW software provides the COCOM with the tools needed to maintain SA, make decisions, direct units, share information, and monitor execution at the scene (see Appendix E for a list of JTCW software). The POP-V itself does not manage the JTCW or the application data, as explained in Appendix E; it simply provides hosting, storage, user interface and display

capabilities. The JTCW software should be installed via a USB or Ethernet interface prior to deployment, as the time required for installation via the Ku band would put a vehicle out of service for a significant duration.

The POP-V delivers a core set of service capabilities to hosted applications and TDSs; these include enterprise services that allow the NOTM to offer access and delivery of information to the COC. The NOTM does not directly connect to the GIG or provide services across the USMC enterprise. It transmits information to and from the COC via satellite and depends on the availability and capability of the transmission system, located at the COC, (MARCORSYSCOM, 2014) for the sharing of information.

The NOTM comprising the above-identified COTS equipment provides an OTM C2 capability that allows the COCOM to extend C2 beyond the range of VHF. With this system, the COCOM can pursue the enemy as rapidly as a vehicle can travel, without the risk of losing communication with subordinate, adjacent, or higher units. Providing a COCOM with a self-forming, self-healing communications network allows for redundancy in areas where the communication infrastructure has been destroyed or did not exist. This capability can potentially fill the communications gap identified by the USMC.

3. Fuel Consumption

There still remains the need to reduce power/fuel consumption (power and fuel are used interchangeably). Manipulating power requirements affects fuel consumption; thus, this research evaluates the power requirements of communications assets to find ways to conserve. By decreasing consumption, the USMC can reduce logistics without degrading C2 and can presumably limit the threat to logistical convoys.

Vehicles conducting logistical resupply are constantly subjected to threats on the road. Reducing fuel consumption at the edge will reduce the number of MTVR vehicles providing support, thus reducing both threat and fuel consumption. The MTVR currently consumes 50% of all ground fuel used by the

USMC (Kelly et al., 2011), so the more vehicles that are off the road, the less fuel consumed.

a. COC CAPSET IV Fuel Consumption

As previously discussed, the COC CAPSET IV is primarily considered an ATH C2 asset, with the capability of providing a mobile jump COC. Organic to the COC are two M1152A1 HMMWVs and two generators that power the main COC and antenna hill. Table 1 provides the characteristics of a M1152A1 HMMWV, according to TM 1103-OR (2012). By evaluating the CAPSET IV power requirement, one can gauge fuel consumption and compare results with similar assets.

As designed, the two M1152A1 HMMWVs have specific tasks. Their primary task is to transport CAPSET IV components during deployment; their secondary is to conduct mobile jump COC operations. Once erected, it is possible to operate a COC without using the HMMWVs, thus reducing overall fuel consumption; however, this option would eliminate the jump capability.

According to the USMC TM 11033-OR (2012), data listed in Table 1, the M1152A1 can achieve ten miles per gallon (MPG). This data is calculated on a vehicle with no payload. However, adding the CAPSET IV's complete payload of 12,705 pounds (per Appendix G) decreases the achievable MPG range (exact data not available).

Figure 10 indicates the power consumption of the CAPSET IV proper in kilowatts (kW) according to iGov (2013). A kW is approximately 1.34 horsepower. When analyzing the total power requirements for the CAPSET IV with the organic 20 kW generator, rate of fuel consumption is calculated to be approximately 4.58 gallons per hour, based on an estimated fuel consumption rate for a 20 kW generator (see approximation chart in Appendix F).

ITEM	SPECIFICATIONS
Width	87 in. (221 cm)
Height	76.25 in. (193 cm)
Length	194 in. (493 cm)
Vehicle Curb Weight	7,100 lbs. (3,221 kg)
Gross Vehicle Weight Rating	12,100 lbs. (5,493 kg)
Vehicle Payload (including Crew)	3,340 lbs (1,515 kg)
Cruising Range	250 miles (402 km)
Alternator	400 ampere
Voltage	28 Volts
Battery	Two, 12 volt (800 CCA ea. At -18 degrees F [-28 degrees C]
Fuel Tank	25 Gallons (94.6 Litters)

Table 1. M1152A1 HMMWV Technical Specifications from the USMC TM 11033-OR (2012).

Figure 10. CAPSET IV Total Power Requirement (from iGov, 2013).

b. NOTM Fuel Consumption

The NOTM suite, unlike the CAPSET IV, is dependent on tactical vehicles throughout deployment. There are a variety of tactical vehicle types in which the NOTM suite can be installed (e.g., Amphibious Assault Vehicles (AAV), HMMWVs, Mine-Resistant, Ambush-Protected vehicles (MRAP) and M-ATVs)

(MARCORSYSCOM, 2014); however, this study evaluates the fuel consumption of the NOTM suite installed in a HMMWV and M-ATV, as these are the vehicles in which NOTM suites are currently installed. Table 2 provides the characteristics of the 1162A1 HMMWV (USMC TM 11033-OR, 2012) and Table 3 provides the characteristics of the M-ATV (USMC TM 11803A-OI, 2013).

ITEM	SPECIFICATIONS
Width	87 in. (221 cm)
Height	76.25 in. (193 cm)
Length	194 in. (493 cm)
Vehicle Curb Weight	7,230 lbs. (3,279 kg)
Gross Vehicle Weight Rating	12,100 lbs. (5,493 kg)
Vehicle Payload (including Crew)	2.230 lbs. (1,012 kg)
Cruising Range	250 miles (402 km)
Alternator	400 ampere
Voltage	28 Volts
Battery	Two, 12 volt (800 CCA ea. At -18 degrees F [-28 degrees C]
Fuel Tank	25 Gallons (94.6 Litters)

Table 2. M1165A1 HMMWV Technical Specifications According to USMC TM 11033-OR (2012).

ITEM	SPECIFICATION
Width	98.0 in. (284.9 cm)
Height	108.9 in. (276.6 cm)
Length	265.1 in. (673.4 cm)
Vehicle Curb Weight	28,500 lbs. (12,940 kg)
Gross Vehicle Weight Rating	37,000 lbs. (16,798 kg)
Cruising Range	320 miles (515 km)
Alternator	570 amp
Voltage	24 volts with 12 volt accessory provision in capsule
Battery	Four, 12 volt (800 CCA ea. At -18 degrees F [-28 degrees C]
Fuel Tank	47 Gallons (177.9 Litters)

Table 3. M-ATV Technical Specifications According to USMC TM 11803A-OI (2013).

According to TM 11033-OR (2012) data listed in Table 2, the M1165A1 can achieve 10 MPG. This data is calculated on a vehicle with a zero payload. With SVK components installed, the payload increases by 620 pounds (USMC TM 12272A-OR/1, 2013) and decreases the achievable MPG (exact data not available). In regard to M-ATV capability, the data listed in Table 3 indicates that the M-ATV can achieve 6.8 MPG. This data was calculated on a vehicle with zero payload. With POP-V components installed, the payload increases by 1,330 pounds (USMC TM 12271A-OR/1, 2013) and decreases the achievable MPG (exact data not available).

In conclusion, the USMC requires a communications asset that can be pushed down to the lowest unit levels operating in an expeditionary environment at the tactical edge. It is apparent that with increased C2 capabilities, there is an increase in fuel requirement. Fueling these C2 capabilities is increasing the burden on logistical trains. To maintain operational capability, the USMC is placing more vehicles on the road to resupply units. In so doing, they are

simultaneously increasing overall fuel consumption within the service and placing more Marines at risk of roadside attack. To break this chain, the USMC needs to explore other communications technologies.

IV. DESIGN MODELS, APPLICATIONS, AND COMPARISONS

This chapter introduces a proposed virtual architecture for an expeditionary C2 system to support units operating at the edge. In previous chapters, system architectures were analyzed to ascertain compliance with MAGTF requirements and user needs. This chapter analyzes the past EOC field experiments conducted by NPS faculty with the Monterey County FRC. The results of the field experiments and salient characteristics of the EOC led to the development of an enhanced EOC called EOC-2. In this research, the models were compared with existing USMC systems for possible development of a new system. The results were used to evaluate whether the EOC models could support small units at the edge. This chapter concludes with a theoretical VM architecture that could potentially support MAGTF expeditionary requirements.

A. SYSTEM REQUIREMENTS

1. Systems Interoperability

As the USMC returns to its expeditionary roots, it is imperative that forward-deployed and tactical-edge units have a C2 architecture that supports the JTCW suite of software (see Appendix E) while at the same time reducing power consumption. The JTCW suite will ensure that the unit's common operating picture is synchronized and integrated. The COCOM's requirement that SA be informed by data gathered throughout the battlefield means heavy reliance on units to push information to higher headquarters rapidly. This information is quickly analyzed, categorized, and displayed via various software products (e.g., CPOF and Adobe Reader—see list in Appendix E) to the COCOM and adjacent and subordinate units to draw a common operational picture. Any communications architecture designed for small units must be able to support JTCW software to access and process collaborative information and reach-back support from higher or adjacent units. This requires the communications

architecture to be interoperable both physically and logically with the already established USMC communications architecture and equipment (Ibatuan, 2013).

The ability to support the JTCW suite does not necessarily mean small units operating at the edge will be required to leverage all aspects of the software simultaneously or have mirror capabilities of the COC in terms of bandwidth and speed; it does mean that the interoperability with current systems must be achieved to transfer data and voice. A major challenge in communications architecture is establishing secure links for transmitting classified information.

2. Security

As the USMC explores COTS technology, it is important to ensure these COTS systems meet DOD security parameters. NIPRNET, SIPRNET and CENTRIX information must be accessible without danger of compromising or spilling information within these networks. According to Hale and Nicely with the Committee on National Security Systems (2013), spillage is the transfer of classified or sensitive information to unaccredited and unauthorized information systems, applications, or media. A data spill indicates classified or sensitive information that is stored on or transmitted over information systems or networks that are:

- Not formally accredited to host or process that information (e.g., secret information to the NIPRNET
- Not formally accredited to host or process information subject to specific restricted handling caveats (e.g., NATO)
- Not formally accredited to host or process information under the control of a particular dissemination-control system
- The inappropriate release of information to a foreign nation

COTS technologies will need firewalls and anti-virus programs, as well as the ability to operate with approved National Security Agency (NSA) encryption devices. Encryption is the process of obscuring information to make it unreadable without special knowledge (Kessel & Goodwin, 2005). According to Kessel and

Goodwin (2005), encryption is the primary means of securing traffic on a network. Valid traffic needs encryption to protect the CIA of each packet. The USMC to ensure information is properly encrypted before dissemination currently deploys a number of devices.

a. SECNET-54 Radio Module

The Harris Corporation (2013) describes the SECNET-54 radio module (RMOD) with its secure, wireless, local-area network (SWLAN) technology as a device that provides secure wireless data, video, and VoIP capabilities. The SECNET-54 is NSA-certified for 802.11a/b/g application, due to its ability to provide type 1, layer 2 (using the RMOD), and layer-3 SWLAN encryption to secure data and network header information for all network layers. The entire packet is encrypted, which prevents adversaries from gaining information from intercepted traffic analysis. SECNET-54 provides secure communications up to the level of top secret/sensitive, compartmented information (TS/SCI) and significantly reduces the bulk of externally wired encryption equipment. SECNET-54 capabilities include virtual private network (VPN) with network address-translation traversal (NAT-T), permitting unfettered operations in COTS equipment. It also includes virtual local-area network (VLAN) tag pass-through without the use of generic routing-encapsulation (GRE) tunnels. It can be configured to allow individual laptops to communicate with each other without an accompanying network infrastructure. Wireless bridges can be used to transmit secure data up to ten miles with the use of external antennas and amplifiers. This capability significantly increases usefulness and application in tactical environments when data can be secured over extended ranges (Harris Corporation, 2013). Figure 11 provides a look at the SECNET-54.

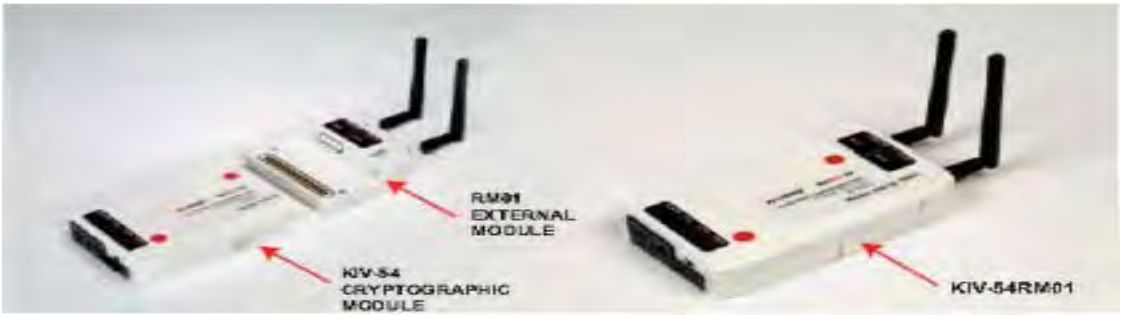

Figure 11. SECNET-54 Cryptographic Module and Radio Module (from Harris Corporation, 2013).

b. KOV-26 Talon Card

The L-3 Communication Systems–East Corporation (2013) identifies the Talon card as an NSA-approved type-I encryptor that allows data access to a level of TS/SCI. It is designed as a multi-interface, high-assurance, internet-protocol encryption (HAIPE) device in a Personal Computer Memory Card International Association (PCMCIA) form factor (Marshburn, 2011). It can provide classified data communications via an 802.11b/g, wired Ethernet, V.90 modem, or an RS-232 connection (L3 Communications Corporation, 2013). According to L3 (2013), the Talon is the smallest encryptor used by dismounted units, weighing only three ounces and offering flexible technology that can be used in an off-the-shelf laptop. It provides voice and data interoperability with other encryption devices, including legacy devices. Figure 12 depicts the components of the KOV-26 Talon card.

Figure 12. KOV-26 Talon Card Components (from L3 Communications Corporation, 2013).

The KOV-26 Talon card accommodates up to fifteen users per card; this can be one user per card on fifteen configured laptops, fifteen users on one laptop, or a combination not to exceed fifteen (Assistant Secretary of Defense for C2, Communications and Intelligence, 1997).

c. Suite B

According to the NSA (2013), the secure sharing of information among DOD and coalition forces down to the tactical level is important, and a method to protect classified information must be established. The software would have to be an interoperable cryptographic product that can be widely disseminated and uses the Advanced Encryption Standard (AES), which protects national-security information systems and the information within these systems.

Suite B is part of the NSA's cryptographic interoperability strategy, which has been proven sufficiently protective of unclassified and classified information, up to the secret level (Law & Solinas, 2011). Most data disseminated in the battlefield is classified at secret or below (Marshburn, 2011), which makes a Suite B-equipped device suitable for use (NSA 2010) within the USMC. This

technology allows layered use of COTS technologies and removes the stringent handling and accountability requirements for type-I controlled cryptographic items (CCI). Since this software provides for layered use of COTS technologies, installing it with current or future COTS products would not be a problem.

B. EOC EXPERIMENTS

Barreto (2011) conducted several experiments to validate the EOC as a concept for the Monterey Country FRC. Table 4 identifies the date, location, and title of the experiments. The EOC experiments were conducted in controlled environments, measuring setup time; software interoperability and power draw for the evaluation of alternative power sources.

Date	Experiment	Location	Event
9/23/2011	1	Monterey, CA	Earthquake Drill
9/24 – 9/25/2011	2 & 3	Salinas, CA	California International Air Show
Undocumented	4	San Francisco, CA	Fleet Week
9/13/2011	5	NPS, Monterey CA	Faculty Event
9/20/2011	6	NPS, Monterey CA	Army Civil Affairs School visitation

Table 4. Experiment Matrix for EOC.

While these experiments were conducted during various times in 2011, most of the data gathered (e.g., regarding interoperability of software and power draw) remains relative to the research of an EMOC model. This is owing to the EOC's compatibility with software operating on Microsoft Windows or an Intel architecture, which is commonly used by the USMC (see appendixes A and E for a list of computer-ware). The two aspects that we explore are the power draw and dimensions (system size and weight). These are important evaluation parameters for the development and deployment of an expeditionary model. By

reducing power draw, which equates to fuel consumption, we can potentially reduce the logistical requirements needed to sustain the equipment. It is also the goal of future models to ensure that dimensions compare with the U.S. Military Standards 1472 F (1989) for the physical characteristics of objects handled by military personnel. These standards, developed by the Military Standard Human Engineering Design Criteria for Military Systems, Equipment and Facilities (1989), define the optimal object for lifting as "an object with uniform mass distribution and a compact size not exceeding 46-cm/18.11-in high, 46-cm/18.11-in wide and 30-cm/11.8-in deep (away from the lifter)", (p. 139). This is important because personnel will most likely move the EMOC manually.

Table 5 identifies the weight and idle power draw per component (Chapter 1, Section C, describes the functions of these components). As shown in Table 5, the total weight of the EOC is above the 174-pound ideal limit for a two-man L-L&C, as defined by the Standard 1472F (1989).

Component	Quantity	Power Draw (Watts)	Component Weight
SKB Roto Rack	1	NA	66.75 lbs.
V3 STRAT 100 Server	1	Left P/S/ 100.15 Right P/S/ 91.82	30 lbs.
Cisco SGE200P Switch	1	20.27	5 lbs.
Cisco WRT400N Router	1	Outside PDU Measuring range, relative < 1 Watt	< 1 lbs.
Raritan PX PDU	1	NA	5.6 lbs.
TRIPP-LITT B021-000-19 KVM	1	18.25	40 lbs.
APC 750VA/480 UPS	1	12.95	41 lbs.
Coraid SRX3500 SAN	1	650 Watts (Manufacturer's Claim)	55 lbs.
Total with and without Coraid SAN	8	244.48 (w/out) 894.40 (with)	188.45 lbs. (w/out) 244.35 lbs. (with)

Table 5. Component Quantity, Idle Power Draw, and Weight of EOC.

The experiments by Barreto (2011) provided in Table 4 demonstrate that the concept of the EOC as an operations center for first responders is viable. The EOC met the compatibility and interoperability requirements of the FRC's current software and hardware systems and proved reliable and mobile; however, the system's energy efficiency was not thoroughly measured. The ability to deploy the EOC rapidly in under two hours was demonstrated in all experiments. Deployment in regard to these experiments consists of unloading the EOC container (Figure 13) and alternative power sources (Figure 14), booting up the system, and establishing a connection via a mobile satellite terminal (e.g., ViaSat, BGAN). These experiments also validated Barreto's (2011) assumption that by relying on a VM infrastructure versus a complete physical infrastructure, the EOC could operate successfully on less power (W/h) than a complete physical system and increase command-center mobility without reducing network performance. It is important to note that the EOC was not fully load tested in any of the experiments in Table 4. The power-draw measurements were derived under normal operations with a maximum of three users accessing the network at one time.

The Table 4 experiments taught several lessons in the area of software configuration based on FRC requirements, which this thesis does not visit because FRC requirements do not match those of the USMC (see software and hardware requirements in appendixes A and E). The specific alternative power sources used during the experiments are also not evaluated. The non-tactical alternative power sources (Solar Stik and a Honda EU2000i Generator) used were not a viable solution for military operations in austere environments, due to non-compliance with tactical standards. By providing the EOC operational power requirements derived from the experiments, the military can evaluate which currently approved alternative power source would adequately support the system.

Figure 13. EOC Transit Case (from Barreto, 2011).

Figure 14. Solar Stik Breeze 100 (from Barreto, 2011).

1. Exploring Results and Finding

a. Configurations

In validating the EOC concept, it was discovered that the VM configurations in regard to the Internet protocol (IP), Internet gateway access, and the domain-name server (DNS) were improperly configured. The EOC's infrastructure depends on a reliable DNS, which by design has at least two networks internally, based on the VM infrastructure. The first network is used to communicate to the physical server(s) that runs the VM hypervisor software and uses a static-IP addressing scheme. The second network also uses static IP for the actual virtual infrastructure (in this case the Microsoft windows server); however, the virtual-desktop machines use dynamic host-configuration protocol (DHCP) for addressing. This became an issue during deployment, as the EOC was originally configured to support the FRC using the NPS network only. The

NPS network provided the system with a non-routable private IP address scheme, which subsequently assigned the server a static IP address from the available private IP addresses. Once the system was deployed and attempted to gain access to an outside network via a non-NPS-networked satellite, the IP address scheme originally assigned to the system was invalidated and failed to register to the new network. This prevented the EOC from pulling services from any satellite.

To solve this problem, a Cisco Wireless-N dual-band router was added, allowing the router to serve as both the internal and external gateway and provide an external DNS, DHCP, and wireless authentication, as well as user authentication for the DNS and active directory (AD) to the VM infrastructure. This allowed the EOC to issue a pool of IP addresses properly throughout the network.

b. Power Consumption

The power consumption of the EOC during these experiments fluctuated depending on the number of users (maximized at three) accessing the server and the laptops drawing power from the system. Consumption ranged from a low of 229.0 W/h to a high of 267.188 W/h without the SAN component installed. With the SAN component installed, the power draw was elevated by 640 W/h. During the experiments, the power requirement spiked to 907.188 W/h with the SAN installed. The SAN, as previously stated, provides the EOC with an additional storage capacity of 12 TBs. The added weight and power consumption of the SAN was found to outweigh its potential benefits, thus rendering it excessive and unnecessary (Barreto, 2011). Upon removing the SAN component, power consumption (minus 640 W/h) and weight (-55 lbs.), were reduced significantly. This modification will be implemented in all future EOC models, beginning with EOC-2. Figure 15 depicts the power consumption of the EOC per experiment (Table 4) measured in W/h with the assistance of the Raritan Power IQ software dashboard (Barreto, 2011). These measurements are

presented with and without the SAN component for comparison value. Note: there are no data measuring power consumption for Experiment 6 (Army Civil Affairs).

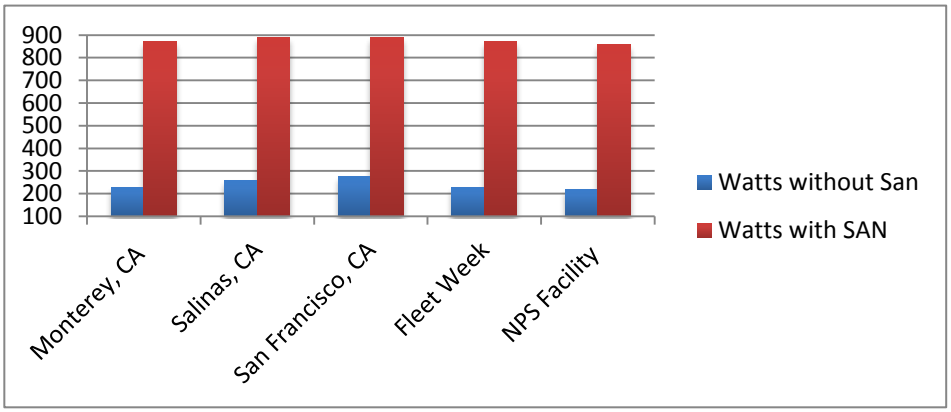

Figure 15. EOC Power Consumption in W/h during Experiments.

It is important to note during the experiments identified in Table 4 that the EOC was not exploited to its full service potential, as the main purpose of the experiments was to validate the concept of the system. The EOC was not load tested with a large number of users connected to the network. Without conducting a load test on the EOC, it is difficult to gauge power consumption during a realistic deployment evolution. The lack of data based on a system-load test skews the power-draw results in Figure 15. This is something to evaluate in a future model.

C. THE INTRODUCTION OF EOC MODEL TWO

With the validation of the EOC concept and the presentation of the results and finding, work began on EOC-2, which would maintain the same communications capabilities as the EOC, in terms of VM functions and networking capabilities, to accommodate the FRC's software and hardware requirements. The main characteristics reviewed for reconfiguration were the dimensions and power draw of the original EOC architecture. An attempt was made to reduce the weight from 244 pounds to 100 pounds and reduce the

power draw from 244.48 W/h to 200 W/h. Reducing the dimensions of the EOC-2 would ensure compliance with commercial-airline standards (foreign and domestic) for cargo dimensions and allow a two-man team to move the system.

1. Characteristics of the EOC-2

The EOC-2 architecture maintains the same structural design elements as the original. However, based on results and findings from experiments on the original EOC, several components were changed. The focus of the EOC-2 model was not only maintaining, but also enhancing the initial criteria of robustness, energy efficiency, two-man portability, and integration into existing HFN infrastructure. Table 6 describes the characteristics and idle power draw of the main components used to create the EOC-2 architecture. See also the data in Appendix I.

Component	Quantity	Power Consumption (Watts)	Component Weight
SKB Roto Rack 28”	1	NA	62 lbs.
Intel Server R1000	1	Left P/S/ 3. Right P/S/128	43.56 lbs.
Cisco SGE2000P 24 Port Switch	1	19.00	5 lbs.
Cradle Point Wireless Router	1	Outside PDU Measuring range, relative < 1 Watt	2 lbs.
Raritan PX PDU	1	NA / NA	5.6 lbs.
Tactical UPS 1.0kva Mobile	1 Separate Case	12.95	77 lbs.
Administrator Laptop	1	.47 / 9.	8 lbs.
Total w/out UPS **Total with UPS**	6 Two cases	152.92	126.16 lbs. 203.16 lbs.

Table 6. EOC-2 Component Quantity, Idle Power Draw and Weight.

By reconfiguring and replacing some of the original EOC components with new COTS technology, Barreto reduced dimensions and power consumption

without downgrading performance. The modifications were made in regard to the server and UPS system. Despite the implementation of new components, the basic functionality remains identical to the original model, although the power draw and dimensions were altered.

a. Power Consumption

One of the main EOC-2 design goals was to reduce the energy consumption thus reducing the resupply requirement. With the new design configuration, the EOC-2 was tested and evaluated to measure power draw, using the following COTS software"

(1) Raritan Power IQ Software

The Raritan Power IQ software suite was chosen to measure the power draw of the EOC-2 in W/h, during all testing. This software worked with a Raritan PDU hardware system in the EOC-2. The Raritan PDU monitors the W/h required as the EOC-2 operates. The Raritan Power IQ software is a free program designed to monitor equipment power draw and distributed breakdown within the EOC-2 architecture. This same software was used to measure the power draw of the original EOC; it is commercially available from the Raritan Corporation (www.raritan.com).

(2) Testing Anywhere Software

The Testing Anywhere software suite was chosen as a way to load test the EOC-2 server. Load testing, for the purpose of this thesis, refers to the simulation of a large number of users accessing the server simultaneously to determine capability. The Testing Anywhere suite is a free software downloaded from the Testing Anywhere website (www.testinganywhere.com) and installed onto the EOC-2 administrator's laptop. The software was used to simulate user activities on the network, allowing researchers to measure the amount of power the server requires to support users.

The Raritan Power IQ software, combined with the Testing Anywhere suite and PDU hardware, provided adequate tools to measure the power draw of

the EOC-2 under simulated real-world use. With these programs installed, the researchers controlled the number of users accessing the network at any given time, thus allowing monitoring of power draw based on the quantity and activities of users.

The researchers began testing by installing Microsoft Windows Server 2008 and 2012 on the EOC-2 server. They recorded the power draw in W/h for the server at one-hour intervals for a range of times. To compute the average power draw, the researchers averaged the power draw during the time frame tested, which varied depending on the testing iteration. Three tests were conducted to measure and evaluate power draw. For these tests, the EOC-2 was configured to accommodate 25 virtual users. Testing allowed all 25 users to access the applications on the EOC-2 server network simultaneously. The number of virtual users was based on a standard-size USMC infantry platoon, per MARCORSYSCOM (2013), and the limitations of the testing software.

All testing was conducted in the Virtual Cloud Lab located in Root Hall on the NPS campus, which is climate controlled to cool other servers not included in this research. This allowed the EOC-2 server's cooling system to operate at a constant 2.35 W/h. To compensate for the artificial cooling of the testing facility, the researchers added an additional 14.45 W/h, derived from the manufacture's published system configurations. These configurations accounted for the cooling system's maximum power draw of 16.80 W/h. The researchers deducted the normal operating power draw of 2.35 WPH (recorded by the PDU) from the maximum power draw published by the manufacture (16.80 W/h), which equaled 14.45 W/h.

Before the experiments, the power draw was taken from the EOC-2 in a standby state. For this research, "standby state" means the EOC-2 is powered on with zero user activity present. The baseline measurement was taken (in watts) using the Raritan Power IQ software over a 24-hour period, for a result of 152.93 W/h. All graphs of the three tests conducted represent the baseline of 152.93 W/h, and the minimum, maximum and projected power drawn based on the

cooling system operating at max capacity (14.45 W/h) for the duration of a given test.

In preparation for the tests, the Testing Anywhere software was configured with the parameters in Table 7. These indicate the number of simulated users accessing the server's various applications and the number of instances in which they occur. An instance, for the purpose of this study, refers to a user's random access of any of the following applications:

- Email
- SQL databases
- Web servers
- Network components
- Applications (i.e., Windows)
- Other installed software

The instances were scheduled to occur continuously during two 12-hour and one 24-hour period. These timeframes were chosen to simulate high user server demand.

Experiment	**Total Users**	**Total Instances**	**Time Frame**
One	25	10,000	12-Hours
Two	25	10,000	12-Hours
Three	25	10,000	24-Hours

Table 7. Defined Parameters For EOC-2 Experiments.

After testing in accordance with the parameters identified in Table 7, the following results were observed and recorded:

Experiment One: The power draw fluctuated between the baseline power draw of 152.93 W/h to a maximum power draw of 218-W/h and 232.35 W/h, incorporating the continuous operation of the cooling system as identified in Figure 16.

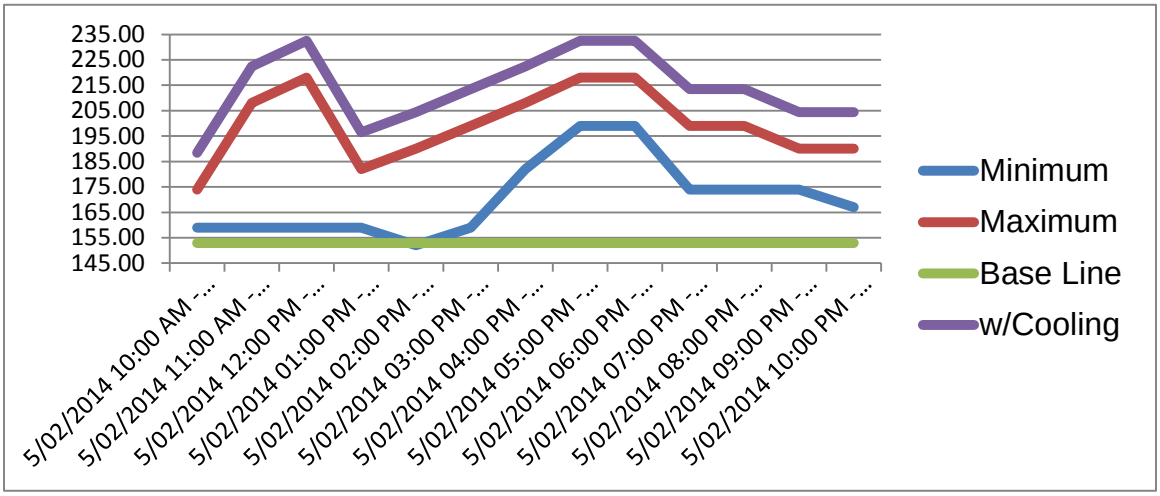

Figure 16. EOC-2 Experiment One: Base Line, Minimum, Maximum and Projected Power Draw Due to the Cooling System.

Experiment Two: The power draw fluctuated above the baseline power at 167 W/h to a maximum power draw of 190-W/h and 204.45 W/h, incorporating the continuous operation of the cooling system as identified in Figure 17.

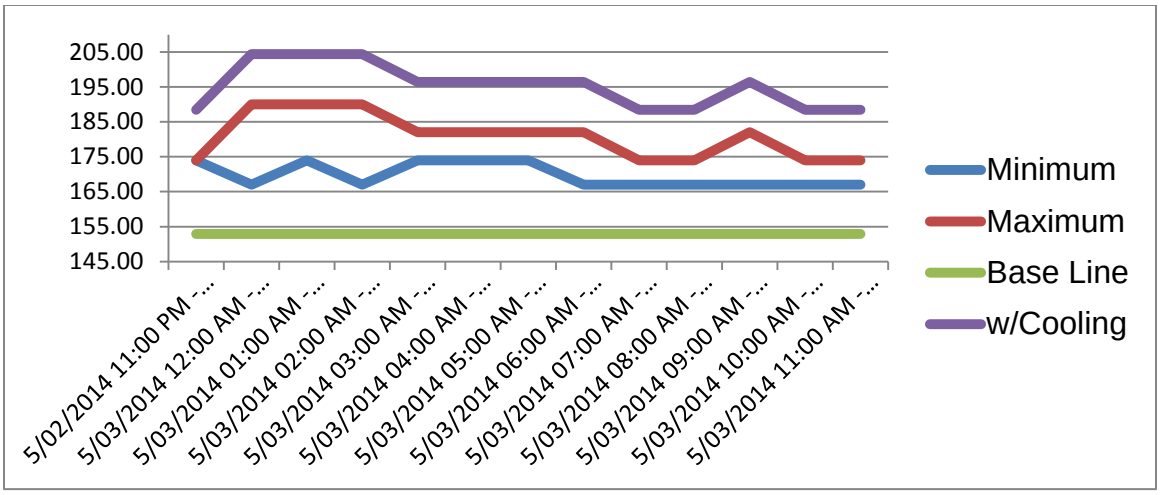

Figure 17. EOC-2 Experiment Two: Base Line, Minimum, Maximum and Projected Power Draw Due to the Cooling System.

Experiment Three: The power draw fluctuated above the baseline power at 167 W/h to a maximum power draw of 190-W/h and 204.45 W/h, incorporating the continuous operation of the cooling system as identified in Figure 18.

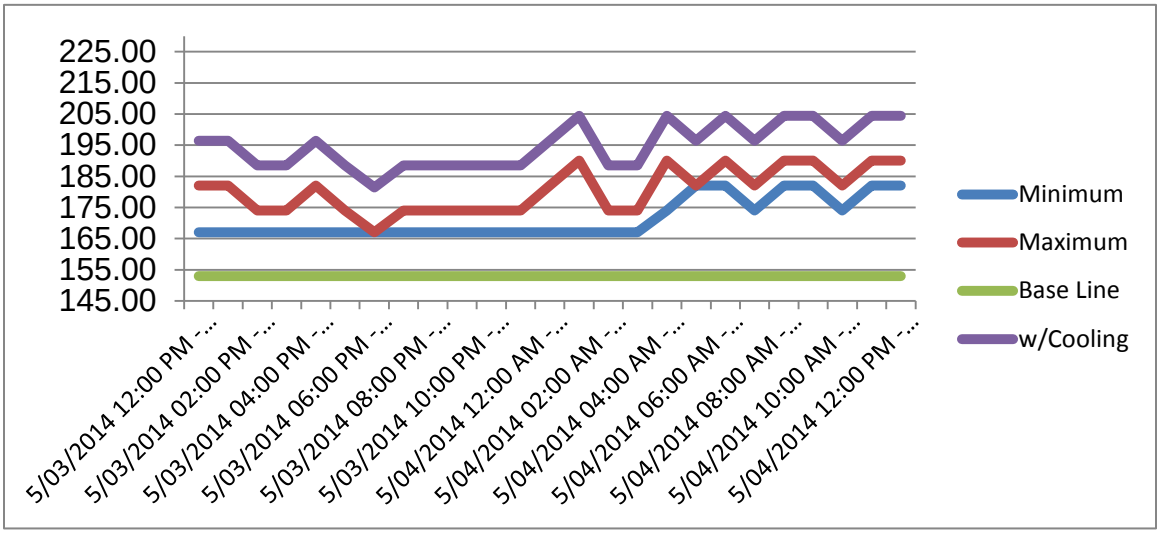

Figure 18. EOC-2 Experiment Three: Base Line, Minimum, Maximum and Projected Power Draw Due to the Cooling System.

During testing the EOC-2's power draw fluctuated between the baseline of 152.93 and a maximum 218 W/h and 232.35 W/h, incorporating the continuous

operation of the cooling system. Figures 16, 17, and 18 were generated using the parameters identified in Table 7 and raw data recorded using the Testing Anywhere and Power IQ software and the EOC-2' PDU (see Appendix H). Recall that an additional 14.45 W/h was added to all totals to simulate the continuous operation of the server's cooling system under torrid conditions.

b. Dimensions

Policies on cargo weight can vary depending on the airline and its location and travel destinations, whether the continental U.S. (CONUS) or outside the continental U.S. (OCONUS). For the EOC-2, we focus on CONUS travel, as the system is designed for the CONUS FRC. For transportation of the EOC-2 within CONUS, one would have to comply with the weight parameters for domestic flights. These standards vary depending on the airline; however, the majority of airlines limit cargo to 100 pounds, which may be exceeded for an additional fee (Wikitravel, 2013). In the research, the design goal of 100 pounds reflects the need to ensure that the EOC-2 is manually transportable by two persons.

Although the Occupational Safety and Health Administration (OSHA) does not have a standard directly related to manual L-L&C the National Institute for Occupational Safety and Health (NIOSH), has developed an equation to determine recommended L-L&C (U.S. Department of Labor, 2014). The equation determines the recommended lifting index, which provides a relative indication of the risk of injury associate with various L-L&C tasks. The equation does not predict the exact risk for injury, but does provide a guideline for the weight one person should lift: 51 pounds (English & Nelson, 2010). This is another guideline that should be used by Barreto to achieve the dimension goal of 100 lbs for the EOC-2. Testing for an EOC-3 is scheduled for late 2014— beyond the timeframe of this thesis.

D. AN EXPEDITIONARY MOBILE OPERATIONS CENTER (EMOC)

With data and experimental testing of the EOC and EOC-2 completed, the design of an EMOC model is proposed to bridge the communications gap at the tactical edge. Table 8 depicts the proposed components for the EMOC design with the same power consumption and component weight characteristics as the EOC-2. Note that this research does not endorse any specific brand or manufacturer of COTS components; nevertheless, the design is based on capabilities and characteristics observed empirically by testing specific COTS components for the EOC-2. In theory, any component meeting the parameters and specifications of the equipment used during testing should produce similar results. Table 8 presents proposed major component and specifications for the EMOC.

Component	Quantity	Power Consumption (Watts)	Component Weight
Ruggized Case	1	NA	62 lbs.
Wireless Router	1	Outside PDU Measuring range, relative < 1 Watt	2.5 lbs.
Encryption device	1	8	12 lbs.
Server System	1	Left P/S/3 Right P/S/ 128	43.56 lbs.
24-Port Switch	1	19.00	5 lbs.
PDU	1	NA / NA	5.6 lbs.
UPS	1	12.95	41 lbs.
Total	6	160.92	171.66 lbs.

Table 8. Proposed Major Component and Specifications for the EMOC.

The characteristics explored for reconfiguration of the EOC-2 to comply with USMC requirements are as follows: security, access to multiple enclaves (SIPRNET, NIPRNET, CENTRIX), lightweight, and energy efficient. These areas were identified to accommodate MAGTF-defined capabilities of secure C2, compatibility with current software and hardware (as detailed in appendixes A and E), lightweight, mobility, and energy efficiency.

The EOC-2 VM configurations are optimal to meet current USMC software and hardware systems and programs. The VM infrastructure is compatible with any Windows or Intel architecture, which is preferred because all software used in the USMC network is so based. The main research focus for reconfiguration to an EMOC concerns security, weight, and energy efficiency.

1. EMOC Security

Security is important in any network architecture, and especially for the USMC. Information is disseminated on one of three enclaves—SIPRNET, NIPRNET or CENTRIX—depending on the classification level. A benefit of operating within the VM architecture is the ability to partition the VM system, allowing multiple enclaves to operate within the same physical server and eliminating the need for multiple physical machines. As explained in Chapter II, this is accomplished through the VM hypervisor. While partitioning is a feature, hosting multiple enclaves on a single VM can introduce threats to the architecture and network clients.

Security for the proposed EMOC architecture was explored in two ways. First was the capability of the architecture to protect against traditional threats, including malware, viruses, rogue security software, Trojan horses, malicious spyware, worms, botnets, and rootkits. The USMC network is configured to help mitigate these threats, at a minimum following the U.S. government configuration baseline guidance, which provides standard Win7 security configurations developed by many agencies (including DISA and the NSA). These basic configurations, combined with firewalls, anti-virus programs, monitoring software,

and other classified capabilities, detect, isolate, and destroy viruses and malicious software. The theoretical EMOC would be protected by these measures, while connected to the USMC network architecture, and by maintaining resident anti-virus software and firewalls for added protection.

The second security aspect explored is a threat to the physical VM architecture via the VMM. The two known threats to the VM architecture, hyperjacking and virtual machine jumping, are discussed in Chapter II. An attack on a VMM allows an adversary to bypass all network defenses and infiltrate all partitioned sections and client machines connected to the VM architecture, maliciously activating network components while remaining completely undetected in the VM architecture. This is possible because the security mitigations lie above the VMM on the OS—these attacks target the VMM, located at the foundation of the VM.

2. EMOC Characteristics

In designing the EMOC, the software and hardware requirements of the USMC, EOC-2 design and capabilities concepts, and U.S. Military Standard 1472F (1989) were used as a guide. With the computerware requirements met using the server system, we focused on meeting the dimension parameters identified in U.S. Military Standard 1472F (referred to as Standard 1472F hereafter) and energy efficiency.

Standard 1472F sets limits on the loads to be lifted by military members, for incorporating into the design of new equipment. The standard sets a maximum load of 174.16-pounds for a two-man L-L&C. Standard 1472F (1989) also identifies the optimal object for lifting, with the assumption that it has handles that are located at half the object's height and 5.9-inches away from the lifter, consisting of "an object with uniform mass distribution and a compact size not exceeding 18.11-in high, 18.11-in wide and 11.8-in deep (away from the lifter)", (p. 139). In addition to meeting Standard 1472F, the researchers wished to meet cargo restrictions in commercial transportation, including aircraft, ground

vehicles, and vessels. Currently, commercial air transportation allows for cargo up to 200 pounds for military personnel (Wikitravel, 2013), which the EOC fails to meet at its current weight. Restrictions that can hinder transportation of an EMOC also exist with some military aircraft (e.g., helicopters) and naval vessels. Thus the proposed EMOC components were researched with weight goals in mind.

a. Ruggedized Case

The proposed container for the EMOC is a 4U ruggedized case similar to that used for the EOC container (a SKB 24-inch 4U Roto Shock Rack). The container provides appropriate shock resistance and measures 27.5-in x 36.75-in x 17-in (length x width x height). Although the width presented exceeds Standard 1472F's 18.11-in by 18.64-in, for a total of 36.75, the benefits of the case override this concern for the researchers. Increasing the width of the ruggedized case by 18.64-in allows the system to maintain all its components together in one case, rather than spread among multiple cases. In addition, the overall weight of the system comes in below the 174 pounds of L-L&C standards.

b. Encryption and Wireless Access Point

The Fortress ES820 self-healing mesh-point system by General Dynamics (2011) is proposed to satisfy the secure communications requirement for the EMOC and converts the EMOC into a SWLAN. The Fortress ES820 is currently used by the USMC with the NOTM suite and has proven reliable (MARCORSYSCOM, 2014). The Fortress' ability to provide secure wireless communications using AES-CTR-128/192/256, AES-GCM-128/256, AES-CCM-128, WPA2 (802.11i), and IPsec (Suite B and Legacy) encryption standards provides it with capabilities similar to the current NOTM suite, as regards wireless access for mesh clients (laptops, tablets, etc.) and secure communication with the USMC network. It also provides the units with flexible maneuverability and a smaller footprint in the expeditionary environment. The Fortress functions as both a wireless access point and a network bridge. Designed as a lightweight and

rugged component with a maximum power draw of 12-W/h (General Dynamics, 2011) it complements the proposed design of the EMOC. This asset enables the unit to form a network spontaneously without preexisting infrastructure, which can potentially save time.

c. Server System

The server system, which was also used in the EOC-2, is a 1U rack-mounted server that combines performance and power efficiency. It contains 128 GBs of RAM, sufficient memory for the execution of the VMware configuration supporting the Microsoft Windows AD infrastructure, VMs, and other applications on the server. This amount of RAM has been demonstrated to support between 25 and 50 VM clients, depending on the RAM allocated to each machine by an administrator. Based on industry standards, a typical 64-bit Windows 7 VM is allocated 3 GB of RAM. This provides enough RAM for partitioning the VM to handle multiple enclaves (i.e. SIPRNET, NIPRNET and CENTRIX) and OSs (Windows, Linux, etc.), reducing the unit footprint by limiting the number of servers required.

This research proposes that the EMOC configuration contain a server system similar to the EOC's, ensuring maximal computing power. To help increase storage capabilities and allow COCOMs flexibility in the allocation of local and host data, or applications on the server, it is recommended that the server be outfitted with eight TBs of SSD local storage. This provides scalability to the server, allowing an increase or decrease of RAM, depending on mission requirements. Similar to the EOC, the proposed EMOC utilizes a VMware ESX or ESXi, for which the USMC already owns licensing privileges. The proposed EMOC architecture includes VMware View and an ESX server as well as the AD, DNS, and other systems that support user authentication, machine identification and validation, and security. This architecture is designed to support up to 50 virtual desktops, accessible through a variety of media (tablets, smartphones, thin clients, zero clients, laptops, etc.) running Windows, Macintosh, or Linux

OSs and providing units at the edge with a complete virtualized environment that mirrors the COC.

d. 24-Port Gigabit PoE Switch

A 24-port gigabit PoE switch is proposed for the EMOC configuration as a redundant method of connecting to the EMOC network. The preferred method of gaining access to the network in an expeditionary environment is through the wireless access point associated with the EMOC architecture. This method allows a decreased footprint by eliminating the need for Ethernet cabling. However, by adding the 24-port gigabit PoE switch, the COCOM maintains the option of having computers connect to the EMOC via Ethernet cable. This can prove beneficial if the COCOM plans to operate in a fixed position for a prolonged period and the footprint size is irrelevant or the wireless access point is degraded. Adding a switch to the EMOC architecture would allow 24 computers to connect directly via Ethernet.

e. Power-Distribution Unit

The proposed EMOC configuration maintains the EOC's PDU component, which lets personnel measure the power consumption of the system with accuracy. This can be beneficial in analyzing which devices use the most power and which systems can be condensed when power needs to be conserved. The PDU also manages the power outlets by allowing the shutdown of unused outlets. This feature prevents prohibited items, such as phones and coffee pots, from drawing power from the EMOC. The PDU also reduces the load on the power system during the booting cycle by allowing power outlets to be staged on and off. The current PDU in the EOC-2 is compact, which allows the PDU and the switch to share a single slot, thus maximizing space in the container.

f. Uninterrupted Power Supply

The proposed EMOC architecture includes a UPS system similar to that found in the EOC, but removed from the EOC-2. The EOC has an APC SMART

UPS 750 mounted in the ruggedized case, which provides 750 watts of backup power. The EOC-2 contains a detached 1000 watt SMART UPS, providing an additional 250 watts of protection. The tradeoff is the backup unit's removal from the ruggedized container and separate housing in its own case (Figure 19), due to its larger size. The benefit is that the COCOM can deploy the EOC-2 with or without the UPS component.

Nevertheless, this research proposes that an internal UPS be housed within the EMOC ruggedized case. The risk of power threats and the stakes of C2 are too high to allow the option of not having an UPS; the EMOC should never be deployed without one. If additional UPS services are required, the COCOM can attach a separate component to the architecture via an outside case, such as that displayed in Figure 19.

The dimensional benefit of removing the internal UPS from the EMOC architecture does not outweigh the potential cost of power failure. Additionally, by incorporating new COTS UPS technology (for example, the Cyber Power system) the EMOC can maintain an internal 1000-watt UPS without significantly increasing weight.

Figure 19. Tactical Power UPS with Ruggedized Case.

g. Energy Efficiency

The proposed EMOC architecture is designed to reduce power consumption by units operating at the tactical edge without degrading C2 capabilities. The EOC was used as a baseline due to the success of Barreto (2011) in reducing power draw and its use of alternative power sources (wind and solar). As currently designed, the EOC's power requirements range from 894.4 W/h (with SAN) to 244.48 W/h (without SAN). The EOC-2 tested has a lower power requirement than the original EOC, fluctuating between the baseline of 152.93 to a maximum 218 W/h and 232.35 W/h, incorporating the continuous operation of the cooling system as identified in figures 15, 16, and 17. The EMOC concept was created to significantly reduce the power draw of a C2 system while meeting USMC needs, thus reducing the fuel needed to operate the system. By reducing the fuel consumption of the EMOC architecture, a unit can potentially reduce the logistical requirement associated with refueling its location.

V. FINDING, RECOMMENDATIONS, LIMITATIONS, AND CONCLUSIONS

A. RESEARCH FINDINGS

The findings of this research as they pertain to the research questions, recommendations, and a conclusion are presented in this chapter.

1. Research Question One

The first research question was, how could the current EOC-in-a-box architecture be modified to reduce weight, improve maneuverability, and still provide the security and C2 capabilities needed to bridge the communications gap?

a. Weight and Maneuverability

Redesigning the EOC's architecture to reduce weight and improve maneuverability is theoretically achieved in the EMOC system design. The modifications, identified in Chapter IV, are based on the original EOC models and EOC-2. The proposed new components for an EMOC model reduce the original EOC architecture from 244 pounds to 159.66 pounds, comfortably below the 174-pound Standard 1472F maximum recommendation for two-man L-L&C. The weight reduction afforded by this configuration is intended to assist the maneuverability of the system. However, since the EMOC is a theoretical design, measurement of system maneuverability in practice is difficult.

b. Security

The EOC concept as currently designed is not a viable option to solve the USMC's identified communication gap, failing to satisfy the MARCORSYSCOM (2012) MAGTF C2 characteristics of interoperability and trust, both in its capabilities and the validity of the information made available.

The EOC's center of gravity is its reliance on virtualization to perform communications and reduce weight and energy consumption, which it effectively accomplishes; however, this virtualization aspect of the EOC is also its critical vulnerability. There is an identified vulnerability in the virtualization of OSs and server partitioning that allows the running of multiple enclaves. This research brings to light the critical vulnerabilities present within the VM hypervisor, which permit a sophisticated adversary to attack the VM without detection, allowing access to all operating systems within the VM. Since the hypervisor operates beneath the OS layer, it may be vulnerable to hyperjacking and virtual machine jumping as well—severely compromising network security and data.

Another shortfall in the EOC is that any network architecture presented as a solution to the USMC communications gap must facilitate all three network enclaves currently used by USMC units: SIPRNET, NIPRNET and CENTRIX. Adding encryption devices to the EOC architecture might in theory support these enclaves, but not with the level of security required by the NSA.

Two factors hinder the EOC from supporting these enclaves: first, VM architecture vulnerability via the hypervisor. The hypervisor vulnerability can potentially allow an adversary access to one or all of the network enclaves, allowing classified information stored in the VM to be compromised. Second, is the "one server" architecture concept of the EOC. As designed, the EOC architecture contains only one server, which in theory would be partitioned to support classified and unclassified networks. Owing to this design, the EOC architecture fails to meet the NSA and USMC's policy on the physical and logical separation, or air-gapping, of different classifications of networks (classified and unclassified). Air gapping is defined by *Technopedia* (2014) as:

> A security measure implemented for computers, computer systems or networks requiring airtight security without the risk of compromise or disaster. It ensures total isolation of a given system electromagnetically, electronically, and, most importantly physically from other networks, especially those that are not secure. (*Technopedia*, 2014, para. 1)

Since all networks would be housed on one server there is the potential for classified or sensitive information to be leaked from a classified to an unclassified network. One way to mitigate this vulnerability would be to install another server in the architecture. This would allow air gapping of the NIPRNET and SIPRNET; however, it would require a larger ruggedized case for the additional server, thus increasing the overall weight of the system by roughly 44 pounds. The weight of the EMOC system would increase from 159.66 pounds to 203.66 pounds, pushing it well beyond Standard 1472F's recommended two-man L-L&C weight of 174 pounds.

c. C2 Capabilities

EOC architecture can physically and logically support all USMC software and hardware requirements identified in appendix A and E—but not in accordance with NSA and USMC security policies. Due to the EOC's inability to meet the NSA and USMC policy on physical and logical separation of classified and unclassified networks, it does not meet accreditation parameters for operating the software and hardware identified. Some of the software and hardware programs identified in appendixes A and E are required to operate on various classified and unclassified networks, depending on function. Since the EOC as designed would only be accredited to accommodate one enclave, supporting the computerware identified is not feasible. Units deploying the EOC concept at the edge, with access to just one enclave (either SIPRNET, NIPRNET or CENTRIX) would not be ideally served, as their communications capability would be limited.

2. Research Question Two:

How can the EOC-in-a-box's energy-efficiency plan be modified to reduce the logistical burden associated with C2?

a. Energy Efficiency

Underestimating power consumption poses a number of risks. If usage exceeds circuit capacity, users run the risk of tripping a circuit breaker and losing power. Users also run the risk of exhausting their fuel supply prematurely, which places an undue burden on logistical units having to resupply them. The key to reducing these problems is deploying assets that are energy efficient and capable of satisfying user requirements. By employing energy-efficient assets, the logistical burden can theoretically be reduced and the opportunity to leverage alternative-energy-producing technology can be enhanced. In evaluating IT equipment for energy efficiency, it is important to consider the environmental conditions in which the equipment will be used. These considerations range from the climate to user activities and may have a huge impact on the power draw of the equipment.

The EOC is considered energy efficient, with a power-draw range of 244.48 to 894.40 W/h (Barreto, 2011). This low power requirement allows the use of solar panels and wind turbines (Barreto 2011) to contribute to operating power. Testing and evaluation of the EOC-2's power requirements reveals a power-draw requirement ranging from 152.93 to 218 W/h, below the minimum range of the original EOC's low point of 244.48 W/h. Taking into consideration the climate-controlled environment in which testing occurred for the EOC-2, the researchers calculated the W/h associated with an EOC-2 cooling system operating continuously. Factoring in manufacturer specifications, this estimation added 14.45 W/h for a maximum power draw of 232.45 W/h. With the additional W/h, the EOC-2 still falls below the original EOC's low point of 244.48 W/h.

The EOC-2's testing parameters were more stringent than the parameters followed during the testing of the EOC, because the original EOC's testing focused on proving the concept. The EOC-2 followed the parameters identified in Chapter IV, Table 7, which called for power draw to be measured with 25 virtual users simultaneously accessing the server. This further validates that the EOC-2's energy efficiency is enhanced as compared to the original EOC. If the

proposed EMOC model is built with components similar to those in the EOC-2, this research suggests it will produce results similar to the EOC-2.

A. STUDY LIMITATIONS

There were several limitations encountered during this study. The EMOC as described in Chapter IV is a theoretical architecture, based on the documented performance of the original EOC (EOC-1) by Barreto (2011) and evaluations and testing of the EOC-2 concept. The EOC-1 is owned and operated by Monterey Country First Responders and could not be made available to the researcher for the purposes of this thesis. We were constrained to rely on past research and assistance from the creator of the EOC concept. Past experiments were documented and cataloged in the areas of dimension and functional concept, which provided a solid background and quantitative data for comparing EOC-1 and EOC-2 for the development of the theoretical EMOC architecture. EOC-1 research did not thoroughly measure or document the power draw of the system with a large number of users. This forced this research to rely on the power measurements of the EOC-2 model only; but we believe that the measurements from the EOC-2 are sufficient to propose an EMOC model, due to the quality of the experiments conducted.

Owing to the lack of CCI (i.e. SECNET 54, KG 175) and security software (Suite B) the EOC-2 was unable to be outfitted with the appropriate computerware. This prevented us from fully testing the ability of the EOC-2 to accept and operate with CCI material. Based on the documented requirements of the security software and hardware, it is theorized that the EOC-2, and by extension the EMOC, would in fact be able to support the software and hardware of these security applications. It is also important to note that the EMOC's proposed design meets the manufacturer specifications for the installation of the security software and hardware.

Testing of the functionality of the JTCW software and the COC's tactical-data systems on the EOC-2 was not conducted, due to lack of the CCI

equipment needed to operate the classified software and an inability to acquire the non-classified software. The research for the theoretical compatibility of software programs for the proposed EMOC design, as identified in appendixes A and E, was based on the program's OS and the ability of EOC-2 to support such programs. As the software identified in appendixes A and E is based on the Windows and Linus OS, the EOC-2 was tested for compatibility and operational constraints in functioning with these OS.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

In conducting this research, we identified several areas that were either out of scope or acting as limitations to assumptions—these should be analyzed in future research. Nevertheless, this research concludes that the EOC concept as designed cannot solve the USMC communications gap at the tactical edge. Further research is recommended in assisting the deployment of the EOC concept for the FRC.

Tactical Alternative-Energy-Producing Technology

Several government agencies are evaluating alternative-energy technology to deploy in austere environments to reduce the consumption of fossil fuels. Once these technologies (for example, solar panels and wind turbines) are identified and refined, evaluating the EMOC under these power sources may assist in further reducing the need for fossil fuels.

Tactical Vehicle Installation

As designed, the EMOC is not configured as an on-the-move architecture. The two limiting factors are its power and transmission (satellite) requirements. The theoretical EMOC draws power via a NEMA 5 connector—an AC-power plug with a three-wire grounding device (hot–neutral–ground) rated for 125 V maximum, with a standard three-prong cable. This research recommends that a prototype EMOC be configured to draw power from a vehicle using the NATO plug receptacle located in many emergency-response vehicles, shown in Figure

20. This would allow the EMOC to be OTM-capable when operated in a FRC vehicle configured with a transmission terminal.

Figure 20. Mini NATO Plug (from Military Battery Systems, 2014).

Hypervisor Security Vulnerability

As previously highlighted, there are security concerns within any virtual machine operating a hypervisor. Further research needs to be conducted on ways to mitigate potential vulnerabilities within the hypervisor, specifically as relates to the threat of virtual machine jumping and hyperjacking. These threats are fairly new to the virtual environment and are only theorized as a threat, but the potential damage would devastate a network, and the problem should be investigated. The idea of an adversary infiltrating a network undetected is cause for alarm, and with this potential vulnerability present in virtual-machines, deploying this type of technology without extensive research is irresponsible.

Extreme-Temperature Evaluation

The FRC can be forced to operate in various climes and terrains during a disaster; thus it is necessary that gear be functional in austere environments. The EOC and the EOC-2 were designed and tested in and around Northern California under ideal weather conditions. This limited the evaluation of the EOC concept for operations in extreme cold and heat. Further research should be conducted on the effects of temperature extremes on the EOC system to determine how it will function in adverse conditions.

A. CONCLUSIONS

This research explores a viable solution to the USMC's communications gap at the tactical edge. The aim is to leverage COTS technology to provide COC-like communication architecture to small units operating in austere environments. The proposed architecture required must be lightweight, energy efficient and allow greater mobility through a reduced footprint and energy consumption. By reducing the energy required for unit communications, this theoretical architecture decreases fuel needs, leading to a reduction in logistical-supply requirements.

The EOC architectural concept is examined as an example of virtualized technology, to determine how such an architecture might satisfy USMC requirements. Server virtualization, HFNs, the functionality of software and hardware in a virtual environment, and the original concept of the EOC architecture are explored. Expeditionary considerations and MAGTF C2 characteristics are also considered, along with current communication architectures, comparing capabilities, weight, and power consumption to determine a baseline for future C2 technology. Finally, the interoperability and security of the EOC are discussed in relation to software and hardware used by the USMC.

Experiments and analysis were conducted on the EOC and EOC-2 for the propose of designing an EMOC communication architecture for use by the USMC, with components, functions, weight and power requirements described. The research suggests that while the EOC concept is not a compatible option for USMC implementation, the EMOC is theoretically viable.

APPENDIX A. SYSTEM RELATIONSHIPS

The table below outlines the most commonly used systems and equipment used by the operating forces within the COC (Headquarters USMC, Combat Development and Integration, 2011).

Type of System	System / POR Name	Mission / Function	Nature of Relationship to COC
TDS / Application	Advanced Field Artillery Tactical Data System (AFATDS)	AFATDS provides an automated capability for fire planning, tactical fire direction, and fire support coordination at the firing battery, fire direction center (FDC), and fire support coordination center (FSCC). AFATDS assists the commander in improving tactical planning and control of supporting arms operations.	Within the COC, AFATDS is primarily used by the Fires Clerk to receive, transmit, edit, display and process fire support requests and store data to facilitate artillery fire support direction and coordination. The Fire Support Coordinator coordinates with the Fires Clerk to plan, coordinate, and control fire support for the commander. The COC does not own AFATDS application software, data, or hardware; it simply provides the power and space to host this software, and facilitates the access to tactical networks.
TDS / Application	AFATDS Effects Management Tool (EMT)	The EMT is a client for the AFATDS. EMT reads information from the AFATDS database and renders this information on a digital map display. This allows the display of unit symbols, battlefield geometries, fire support coordination measures, and target symbols. The EMT allows for data 'drill down' on the objects to interrogate them and display information maintained within AFATDS.	The EMT client is installed on a laptop that is hosted within the COC and connects to the COC LAN and WAN to pull information from an authoritative AFATDS database. The COC does not own EMT application software, data, or hardware; it simply provides the power and space to host this software, and facilitates the access to tactical networks.

Type of System	System / POR Name	Mission / Function	Nature of Relationship to COC
TDS / Application	Command and Control Personal Computer (C2PC)	C2PC provides map overlays, friendly unit locations with status and plans of intended movement, and hostile unit locations. C2PC is linked together within the COC via a Local Area Network (LAN) allowing rapid information exchange between staff sections, and they are also linked with adjacent, subordinate, and higher headquarters via a Wide Area Network (WAN). C2PC has multiple injectors that allow modular systems with an interface with other capabilities such as AFATDS through the EMT.	C2PC serves as a COC Common Operating Picture (COP) application, which typically requires a dedicated, knowledgeable Marine operator using an Intelligence Operations Workstation (IOW) computer connected to an Intelligence Operations Server (IOS) that is often hosted on the COC Operational Trailer. C2PC will be used by the Common Tactical Picture (CTP) operator, as well as other staff principals within the COC to conduct C2. C2PC can still be utilized while connectivity is down showing the last updated COP/CTP, while CPOF terminals cannot.
TDS / Application	Command Post of the Future (CPOF)	The Command Post of the Future (CPOF) is a C2 software system that allows commanders to maintain topsight over the battlefield; collaborate with superiors, peers and subordinates over live data; and communicate their intent. It is decision support systems that provide SA and collaboration tools for the commander to support decision making, planning, rehearsal, and execution management down to the battalion-level.	Similarly to C2PC, CPOF is used as a system that provides a view of the COP. As a decision support system that provides SA and collaborative tools, CPOF is used by the CTP Operator and staff principals to conduct operations. The Marine Corps currently uses CPOF due to specific theatre requirements set forth by Operation Iraqi Freedom (OIF) Combatant Command (COCOM). The Marine Corps uses this system as a collaborative tool to be interoperable with sister services. CPOF is currently a theatre maintained system and is employed as the primary collaboration and staff planning tool at the battalion and above level within unit CPs.
TDS / Application	Force XXI Battle Command Brigade and Below – Blue Force Tracker (FBCB2-BFT)	FBCB2-BFT is a communication platform designed for commanders to track friendly and hostile forces on the battlefield, as well as all known battlefield obstacles. It increases a vehicle commander's situational awareness of the battlefield by gathering information graphically instead of collecting reports verbally. It is a battle command information system designed for units performing missions at the tactical level.	FBCB2-BFT will be employed by the regimental COC, battalion COC, each company COC, and convoys and/or patrols traversing throughout the AO. BFT provides data on battlefield forces that will be projected onto the COP to enable the Commander and staff principals to make informed C2 decisions.

Type of System	System / POR Name	Mission / Function	Nature of Relationship to COC
TDS / Application	Intelligence Operations Server (IOS)	The IOS features GCCS software giving Marine intelligence analyst access to query, update locally and display the Modernized Integrated Database (MIDB). IOS provides automated support to the COC by providing map displays with overlays, friendly unit locations with status and CTP. Marine analysts have the capability to fully integrate locally produced tactical intelligence with theater and national intelligence and display operationally relevant data graphically within the CTP. The IOS is linked with adjacent, subordinate, and senior commands via a WAN. IOS provides an automated message format and a capability to generate and validate variable Gateways to populate the CTP.	The IOS package is installed on a server hosted within the COC and connects to the COC LAN and WAN to pull information from both GCCS and MIDB. The IOS enables the C2PC client to link with the Intelligence Analysis System (IAS) family of systems to receive and process updated intelligence information. IOSv1 provides automated support to the COC at the regiment and above. The IOSv2 is Unix-based and the IOSv3 is MS Windows-based (versions deployed vary depending on the model of the COC units are fielded). The Intelligence Operations Workstations (IOWs) are the equipment suite, which provide automated support to the COC via C2PC.
TDS / Application	Global Command & Control System – Joint (GCCS-J)	GCCS-J incorporates the force planning and readiness assessment applications required by battlefield commanders to effectively plan and execute military operations. Its Common Operational Picture correlates and fuses data from multiple sensors and intelligence sources to provide warfighters the situational awareness needed to be able to act and react decisively. It also provides an extensive suite of integrated office automation, messaging, and collaborative applications.	GCCS-J applications are hosted within the COC on the OT. Applications are accessed either as clients on COC workstations or via the COC LAN or WAN (through TDN). GCCS enhances the operational commander's warfighting capability and aids in the decision-making process by receiving, retrieving, and displaying information to allow warfighters to plan, coordinate, exercise, execute and evaluate marine and joint operations. The COC does not own the GCCS software or hardware; it simply provides power and space, and facilitates access to tactical networks.
TDS / Application	Global Combat Support System – Marine Corps (GCSS-MC)	GCSS-MC is a commercial, off-the-shelf, Oracle-based system that is replacing multiple supply and maintenance legacy systems with a single web-based information system.	GCSS-MC will be primarily used by maintenance and supply personnel for inventory management, supply requisition and maintenance support tracking. The COC does not own GCSS-MC software, data, or hardware; it simply provides the power and space to host this software, and facilitates the access to tactical networks.

Type of System	System / POR Name	Mission / Function	Nature of Relationship to COC
TDS / Application	Joint Automated Deep Operations Coordination System (JADOCS)	JADOCS is a joint mission management software application. JADOCS enables the Joint Force Commander, Component Commanders and supporting tactical-level forces to conduct operational- and tactical-level fires across the entire engagement spectrum. JADOCS provides an integrated set of functional capabilities for data analysis and management, mission planning, coordination and execution of a variety of joint tasks.	JADOCS provides horizontal and vertical coordination within each echelon of the command. Within the COC, this software application used to present and manipulate information pulled from other C2 systems in planning and executing operations, including ground and air coordination. JADOCS is employed within the COC at the Regiment and above.
TDS / Application	MAGTF Logistics Support Systems (MLS2)	MLS2 provide request for services to fulfillment visibility within the COC.	MLS2 are primarily used by maintenance, supply, and distribution end-users to maintain visibility and work request for services until completion. The COC does not own MLS2 application software, data, or hardware; it simply provides the power and space to host this software, and facilitates the access to tactical networks.
Services	User Access	The ability to access user defined DoD Enterprise Services through a secure single entry point.	
Services	Collaboration	The ability to conduct synchronous and asynchronous communications and interaction across the enterprise, including voice, data, video, and manipulated visual representation.	Collaboration enables the Marine Corps and the COC a variety of services to include being able to participate in web conferencing, instant messaging, application sharing and white-boarding.
Services	Content Discovery	The Discovery Service should allow individuals and systems and services to publish and/or advertise information, for an automated system to discover information, and for users and systems to dynamically search that repository of discovered information.	The Discovery Service will improve worker productivity by breaking down information silos and making relevant information across the LAN/WAN and MCEN available quickly and easily.
Services	Content Delivery	The ability to accelerate delivery and improve reliability of enterprise content and services, by optimizing the location and routing of information.	
Services	Enterprise Messaging	The ability to perform electronic messaging between users and organizational entities across the enterprise, including providing customer support.	The Messaging services also supports message queuing and/or messaging passing; this provides an extremely easy and popular method of integrating and connecting warfighting and business applications and legacy systems in heterogeneous environments.

Type of System	System / POR Name	Mission / Function	Nature of Relationship to COC
Services	Directory Services	The ability to provide, operate, and maintain a global directory of users, to include directory synchronization with other lower-level systems and information integrity.	
Networking System	Tactical Data Network	TDN provides a complete integrated data network that forms the backbone of MAGTF data and Defense Message System (DMS). TDN consists of a network of Gateways and DDS interconnected with one another and their subscribers via a combination of common user long-haul transmission systems, local area networks, single channel radios, and the switched telephone system.	The TDN Gateways and DDS equipment provide COC users with the networking capabilities to establish and maintain data connections with other COCs, other centers (logistics, intel, aviation, etc.) and the supporting establishment. Operational equipment that is hosted on the COCs Operational Trailer interfaces to the Gateway or DDS equipment which then provides a direct interface to transmission systems. Data flows and exchanges going across the TDN and DDS are unique to each hosted TDS and application.
Networking System	Data Distribution System - Modular (DDS-M)	The DDS-M connects Marines to essential tactical networks wherever they deploy using advanced communication and networking technologies.	See above.
Networking System	Transition Switch Module (TSM)	The TSM provides the functionality of multiple systems in a transit-cased configuration, local and remote subscriber access, circuit switching and multiplexing, a call service function, transmission multiplexing, transmission security, and a manual patching capability for deployed forces.	The TSM provides the voice telephone (Red Switch and Defense Switch Network (DSN) access and Voice over IP (VoIP)) services to users in the COC.
Transmission Systems	Single Channel Radios (SCR)	SCR equipment includes hand-held, manpack, vehicle-mounted, ground-mounted, and shelterized radios operating in the high frequency (HF), very high frequency (VHF), and ultrahigh frequency (UHF) bands. It also includes TACSAT radios in the UHF band.	The COC is dependent on the availability and capability of transmission systems. The COC can connect through multi-channel radio (MCR) and single-channel radio (SCR) systems to establish voice and limited data networks with higher, subordinate, and adjacent commands. Radio assets are the responsibility of the unit.

Type of System	System / POR Name	Mission / Function	Nature of Relationship to COC
Transmission Systems	Multichannel Radios	Multichannel radio provides the communications links for the switched backbone. It permits multiple users to access a single communications path and includes terrestrial and satellite radio systems. Multichannel radio provides worldwide connectivity through links to the DISN and the links for long-distance communications within the theater and the MAGTF.	See above.

Table 9. Systems and Equipment Used by the Operating Forces within the COC (Headquarters USMC, Combat Development and Integration, 2011).

APPENDIX B. COC CAPSET IV COMPONENTS LIST

The table below identifies the major components of the CAPSET IV (Headquarters USMC, Combat Development and Integration, 2011).

APPENDIX B. COC COMPONENTS LIST – CAPSET IV (Serial Numbers F4254 – F4999)

Figure No.	Figure Title	
0	MAJOR COC COMPONENT GROUPS	
1	COC COMMON MODULE (INCLUDES: OPERATIONAL TRAILER ASSEMBLY 1A1, STORAGE CASE ASSEMBLY, 8 LAPTOP, SLING (PN 300-00170))	
2	ANTENNA HILL KIT, CAPSET IV, SPIRAL I	
3	GENERATOR/ECU/TENT TRAILER (GETT) ASSEMBLY COMPONENTS	
4	GETT ASSEMBLY 1A2 (P/N 01-P54301E001)	
5	OPERATIONS FACILITY (TENT) (OPFAC) ASSEMBLIES - TRANSIT CASES AND TENT CABLES STORAGE CASES	
6	OPFAC PERIPHERALS - STORAGE CASES	
7	BASE-X TENT SYSTEM AND COMPONENTS (LARGE TENT, MODEL 305 TAN)	
8	BASE-X TENT SYSTEM AND COMPONENTS (GARAGE TENT, MODEL 303 TAN)	
9	TENT COMPONENTS	
10	OPERATIONAL TRAILER ASSEMBLY, 1A1	
	OPERATIONAL TRANSIT CASE ASSEMBLIES	PART NUMBER
11	DSU-1 OPERATIONAL TRANSIT CASE ASSY, 1A1A9	01-P54376E001
12	DSU-2 OPERATIONAL TRANSIT CASE ASSEMBLY, 1A4 (1A6)	01-P53841E001
13	DVD RECORDER OPERATIONAL TRANSIT CASE ASSEMBLY, 1A1A13	01-P54339E001
14	HILL SWITCH OPERATIONAL TRANSIT CASE ASSEMBLY, 1A5	01-P54361E001
15	JUPITER OPERATIONAL TRANSIT CASE ASSEMBLY, 1A1A12	01-P54372E001
16	RAID OPERATIONAL TRANSIT CASE ASSY, 1A1A11	01-P54365E001
17	REMOTE SITE SERVER (RSS) OPERATIONAL TRANSIT CASE ASSY, 1A47	01-P54241E002
18	SIPR TX OPERATIONAL TRANSIT CASE ASSY, 1A1A1	01-P54230E001
19	SIPR/NIPR DATA OPERATIONAL TRANSIT CASE ASSY, 1A1A2 (1A1A10)	01-P53496P001
20	TENT SWITCH OPERATIONAL TRANSIT CASE ASSY, 1A1A3 (1A1A4, 1A14)	01-P54368E001
21	UPS OPERATIONAL TRANSIT CASE ASSEMBLY, 1A8	01-P51730D001
	STORAGE CASE ASSEMBLIES	PART NUMBER
22	STORAGE CASE ASSY, 8 LAPTOP	01-P54336E001
23	STORAGE CASE ASSY, ADMIN LAPTOPS, CAPSET IV	01-P54337E002
24	STORAGE CASE ASSY, ANTENNA HILL COMPONENTS, CAPSET IV	01-P53746E001
25	STORAGE CASE ASSY, CABLE SET, MAIN TENT, CAPSET IV, SPIRAL I	01-P54080E001
26	STORAGE CASE ASSY, COLOR PRINTER	01-P53762E001
27	STORAGE CASE ASSY, COPIER	01-P54363E001
28	STORAGE CASE ASSY, CPOF MONITORS AND CABLES, CAPSET IV	01-P54253E004
29	STORAGE CASE ASSY, IP PHONE	01-P53791E001
30	STORAGE CASE ASSY, MEDIUM PRINTER	01-P53783E001
31	STORAGE CASE ASSY, PA SYSTEM, OUTDOOR, 1A59	01-P54117E001
32	STORAGE CASE ASSY, PROJECTOR (1 PROJECTOR, CAPSET IV)	01-P54374E002
33	STORAGE CASE ASSY, SCANNER	01-P54335E001
34	STORAGE CASE ASSY, SHREDDER	01-P53763E001
35	STORAGE CASE ASSY, SINGLE USER WORKSTATION	01-P53747E001
36	STORAGE CASE ASSY, SMART BOARD	01-P54382E001
37	STORAGE CASE ASSY, UPS BATTERY	01-P53799E001
38	STORAGE CASE ASSY, USB AUDIO ADAPTER	01-P54347E001

Table 10. Major Components of the CAPSET IV (Headquarters USMC, Combat Development and Integration, 2011).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. CAPSET IV, PDU POWER CIRCUITS

The below table identifies the CAPSET IV Component's power consumption as monitored by in-line ammeters (Headquarters USMC, Combat Development and Integration, 2011).

Capset IV — PDU Power Circuits Monitored by In-Line Ammeters

Configuration Item	Components	PWR Voltage	Avg PWR	Max PWR	Qty	Estimated Amperes (See Note)	PDU Non UPS Circuits		GETT Utility Outlet Amperes (not monitored)	PDU UPS
							Phase 1- J25 (CB18) Amperes	Phase 1- J27 GFCI (CB18) Amperes		J22 UPS (CB17) Amperes
Tent Switch Transit Case	Switch/Media Converter	120 VAC	102	200	1	0.85				0.9
Admin Laptop	Laptop Computer	120 VAC	72	110	2	0.60		1.2		
Workstation			77	115	8	0.62				5.0
	USB Light	(int)	5	5						
	Laptop Computer	120 VAC	72	110		0.60				
Jackbox	Jackbox	120 VAC	10	20	8	0.13				1.0
UAA Station	Laptop/UAA	120 VAC	80	125		0.67				4.0
Color Printer	Printer	120 VAC	45	65	2	0.54	0.5			0.5
Medium Format Printer	MF Printer	120 VAC	45	65	1	0.54	0.5			
Scanner	Scanner	120 VAC	43	43	1	0.36	0.4			
Shredder	Document Shredder	120 VAC	90	450	1	2.80			2.8	
Projector	Projector	120 VAC	240	265	1	2.00				2.0
Copier	Copier	120 VAC	100	828	1	5.18			5.2	
Tent Lights (Base-X 305)		120 VAC	125	125	1	1.04	1.0			
Emergency lights		120 VAC	75	75	1	0.42				0.4
Interactive Whiteboard		120 VAC		30	1	0.25	0.3			
Tent Lights (Base-X 303)		120 VAC	25	25	1	0.21	0.2			
TOTALS (Amperes)							3.0	1.2	8.0	13.8

NOTE 1: These Estimated Ampere values are meant to show relative maximum power usage of different equipment under stable conditions (without considering power factor).

Where Avg power is significantly less than Max power, the Estimated Amperes value was calculated using 75 percent of Maximum power – typically, not all equipment will be consuming maximum power at the same time (i.e., shredder, copier).

Table 11. CAPSET IV Component's Power Consumption as Monitored by In-Line Ammeters (Headquarters USMC, Combat Development and Integration, 2011).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. COC CAPSET IV IT EQUIPMENT

The table below identifies the type and quantity of the IT equipment for a COC CAPSET IV (Headquarters USMC, Combat Development and Integration, 2011).

		(V)4	
Network Access	SIPRNet	1	
	NIPRNet	1	
	Coalition	n/a	
	NGO	n/a	
Servers	Windows Server	4	
	UNIX/Linux Server	n/a	
	Video Server	1	
	DSU-1	1	
	DSU-2	2	
	ACU-1000	n/a	
	Mass Storage	SIPR 5.4 TB raw (1 model varies) NIPR - n/a Coalition - n/a	
	Switches	4 3 - SIPR 1 - NIPR Coalition - n/a	
	Routers	2 1 SIPR 1 - NIPR	
Transit Cases	Storage Case Assemblies (Hard/Soft)	30	
	Transit Cases	15	

Table 12. IT Equipment for a COC CAPSET IV (Headquarters USMC, Combat Development and Integration, 2011).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E. JTCW SOFTWARE

The table below identifies the Joint Tactical Common Workstation (JTCW) software associated with the NOTM system suite (MARCORSYSCOM, 2014).

Application	Description
COTS	
7-Zip	7-Zip is a file archiver with a high compression ratio.
ActivClient	Allows the DoD agencies to easily use CAC smart cards for a wide variety of desktop, network security and productivity applications. ActivClient CAC enables usage of PKI certificates and keys on a CAC to secure desktop applications, network login, remote access, web login, e-mail and electronic transactions.
ActivePerl	Scripting engine for Perl required by C2PC and ICSF to execute Perl scripts.
Adobe Reader	Allows users to view Portable Document Format (PDF) files.
Adobe Flash Player	Creates rich Internet apps and streaming video and audio.
Adobe Flash Player Plugin	
ArcGIS ArcIMS	Delivers dynamic maps and GIS data and services via the Web. Provides a highly scalable framework for GIS Web publishing. Provided by and used by JEM.
ArcGIS Engine	Allows ArcGIS functionality for C2PC.
CDBurnerXP	Provides CD and DVD burning and duplication capabilities.
Cisco IP Communicator	Allows VOIP calling
Cisco IP/TV Viewer	Permits viewing of video in COC environments.
Cortona VRML Client	A Web 3D viewer that allows for the viewing of VRML file formats.
Converber	Converber is a unit converter. It is a powerful software utility that will help make easy conversions between 1324 various units of measure in 38 categories.
DirectX	Application Programming Interfaces (APIs) built into Microsoft Windows operating systems.
Go Global	Provides remote access to UNIX/GCCS systems.
HP Quick Launch Buttons	This feature is designed to give the operator the liberty of switching screens when holding down the "fn" key and pressing F4. The F9 & 10 (Brightness) keys require a fix to give the operator the liberty of selecting how bright or how dim he needs his or her screen to display. Only applies to HP systems.
i2 Chart Reader	A web-enabled software tool that presents analytical findings.
Internet Explorer	Web Browser
JDK 5	Java Development kit provided and used by multiple applications within JTCW.
JRE 5	Java Runtime Environment (JRE) Update provides libraries, Java Virtual Machine, and other components to run applets/applications written in the Java programming language. Includes Java Plug-in to enable applets to run in popular
JRE 6	
JBoss	Enterprise middleware provided and used by JEM to deploy web applications.
McAfee Agent	DOD Host Intrusion Prevention system that monitors and blocks intrusions by combining signature and behavioral protection with a system firewall. The Defense Information Systems Agency (DISA) uses McAfee's HIP agent to enforce ePolicy Orchestrator (ePO) policies that are managed by DISA ePO servers. McAfee's HIP agent allows the ePO servers to keep client systems up to date with automatic signature updates, security policy updates, and monitor each system's security status.
McAfee AntiSpyware Enterprise Module	HBSS module
McAfee DLP Agent	
McAfee Host Intrusion Prvention	
McAfee Policy Auditor Agent	
McAfee VirusScan Enterprise	Antivirus protection software
MDAC	Contains core Data Access components such as the Microsoft SQL Server™ OLE DB provider and ODBC driver.
Microsoft .NET Framework 1.0	Allows .NET applications to run within JTCW.
Microsoft .NET Framework 2.0	
Microsoft .NET Framework 3.0	
Microsoft .NET Framework 3.5	
Microsoft Office Professional	Provides office productivity applications.
Microsoft SQL Server	Lightweight and embeddable version of SQL Server
Microsoft SQL Server	

Microsoft Windows Media Player	Default media player included within Microsoft Windows XP
Microsoft Windows Professional XP	Operating system for JTCW
Microsoft XML 4	Update to the M crosoft XML libraries
mIRC	Internet Relay Chat Program
Mozilla Firefox	Approved Web Browser to interface with GCCS
Mozilla Thunderbird	Open source email client maintained by Mozilla, similar to Outlook but with support for newsgroups
NX Powerlite	Office document compression utility
Paint .NET	Paint.NET is free image and photo editing software for computers that run Windows. It features an intuitive and innovative user interface with support for layers, unlimited undo, special effects, and a wide variety of useful and powerful tools.
PuTTY	Provides Telnet and SSH capabilities.
Real VNC	Remote desktop client required by COC displays
RemoteView Reader	Display, processes, and analyses remote sensing images and cartographic data.
SMART Notebook	Allows interaction with SMART Board (white board) hardware.
Snag-It	Captures and edits screenshots.
Spark	XMPP Jabber client for instant messaging
Symantec Ghost Client	Symantec Ghost Client (on recovery media only, not on system) creates full backups of PC contents, restores individual files or entire hard drives, monitors and optimizes backup disk space, and encrypts backups to help keep them secure.
VLC Media Player	Multimedia player for various audio and video formats (MPEG-1, MPEG-2, MPEG-4, DivX, mp3, ogg, ...) as well as DVDs, VCDs, and various streaming protocols
X1 Desktop Search Utility	A desktop search utility
GOTS	
AccessNet	Provides VoIP capabilities to interface with the COC.
AMT	Allows for automated mission reporting.
ACID	With ACID, system administrators can configure predefined roles, i.e., subsets of applications, and load them onto workstations.
JTCW Client	Windows-based client software application designed to facilitate military command and control functions by improving Situational Awareness (SA) and to enhance operational and tactical decisions.
CJB	Allows API to communicate with 3rd party JAVA applications.
Commando Light	Displays brevity codes.
JTCW Gateway	Allows users to link-up onto the same network and provides the capability to share a COP amongst other information.
NSI	Used for C2PC Gateway for connectivity to IOS V1 COP Server. ICSF version 4.5.2.x
NSI Patch	
Integrated C41 System Framework	Used for C2PC Gateway for connectivity to IOS V1 COP Server. ICSF version 4.5.3.x
JTCW C & GW Core Application Extensions	
C2Collaboration	Allows for Collaboration within JTCW C & GW
DSTB	Allows import, manipulation, and analysis of terrain data.
C2PC 3rd Party Application Extensions	
AODB	Provides visualization of the Air Battle Plan and Airspace Control Order tasking within the C2PC map environment.
CLC2S Engineering Application Extension	Provides graphic representation of engineering projects as well as obstacles.
CLC2S Logistics Application Extension	Provides graphic representation of mission plans.
CoT	Communicates time sensitive positions: "What, When, Where" (WWW) information. Bundled with CLC2S Logistic Injector & UAV Plot.
EMT	Interface into AFATDS for fire support
JDH	Requests US Army PASS/DDS topics and overlays from the NRTS Client and displays the data on C2PC.
JWARN	Provides an accurate series of information and hazard templates to be used after events involving the offensive use of Weapons of Mass Destruction (WMDs), terrorist use of WMDs, and accidental or intentional releases of NBC or Toxic Industrial Material (TIM).

MOE	Performs basic cata assessments in the timeliness, accuracy, and completeness of the Common Tactical Picture (CTP) being maintained in C2PC.
SPEED	Supports USMC tactical communications systems planning, engineering, and evaluation processes.
C2ERT	Provides a single access point to various documentation, training reference, and publication sources.
CMP	Handles VMF messages
CPA	Assists in the programing of radios
DPVS 2000	An address book for plain language addressing (PLA)
HCI	Assists in the programing of radios
I3 Imagery Applications	
BEAJAR	Bundles files into a single Java Archive (JAR) file and maintains the directory structure.
GOE	GCCS Operating Environment segment
ITS Admin	Provides I3 administrator capabilities.
JIVE	Provides image and video viewing and exploitation application. Provides the ability to display, manipulate, annotate any NITF, GIF and JPEG image cataloged by the ITS Server or from the file system.
JMU	Supports fundamental areas within the JMTK environment. Provides access to common mapping, charting, Geodesy and imagery.
UDIE	Provides standardized imagery import/export services as well as providing a user interface for the imagery transformation utilities (IMX). UDIE provides an application which allows imagery on the ITS server to be converted.
XIS	Directly captures the structure and relationships of data.
JBV	A 3-D visualization tool that provides the user with a whole earth representation, utilizing imagery overlay.
JEM	Models and simulates the effects of Chemical, Biological, Radiological and Nuclear (CBRN) weapon strikes and incidents.
JFRG II	Joint Force Requirements Generator (JFRG II) is a software application designed to provide the joint services with a state-of-the-art, integrated and deployable Automated Information System (AIS) that supports strategic force movements within the mandated 72-hour timeframe. JFRG II provides rapid force list creation and interfaces with JOPES, TC-AIMS II, MDSS II, and the WRS.
JCC	Helps the user configure JTCW, checks for common configuration mistakes such as not changing the hostname
JSBC	Controls all of the security banners on JTCW
JTCW Security Log Monitor Service	Monitors security log file size.
JTCW Route Convertor	Converts RT3 to CRD and CRD to RT3 formats.
JVURM	Logs track and overlay volume and rate change.
JTCW User State Migration Tool	Helps the user migration data between builds, backs up the following: Host File, address book, map data, overlays, messaging, routes, Gateway setup including, user accounts and track groups
MarineLink	A data mining application that queries the following data sources: ASA-L, BAT, C2PC Overlays, C2PC Tracks, DAFIF, Event Tracker, Exchange Public Folders, Gazetteer, IPL, ITSWEB, Local Map Server, MIDB, and MNCI SIGACTS.
PFPS Suite	Provides both pre-mission and post-mission flight planning capabilities.
AR Tool	Creates and saves air refueling tracks or anchors.
BAM	Displays BAM Avoidance Areas and Birdstrike Incidents graphically in FalconView.
CAPS	Calculates Computed Air Release Points (CARPs) and High Altitude Release Points (HARPs) based on the standard ballistic computation formats used for low and high altitude airdrop as defined within the AFI 11-231.
CFPS	Provides accurate flight plans for a variety of missions.
CRD Tool	Allows the exporting of flight route information (files saved with the extension of *.rte) from PFPS to the standardized Common Route Definition file *.crd, and importing *.crd files into a *.rte.
FalconView	Creates, edits, saves, and opens routes. FalconView and the other components of PFPS provide synchronized route editing through the use of a common Route Server.
FalconView Threat Update Tool	Edits the unclassified THREATDB.PRM database, Icons, and the DEFICON.MAP file.
GeoRect	Converts a bitmap (.bmp), Joint Photographic Experts Group (.jpeg), or Tagged Image File Format (.tiff) file into a GeoTiff file which can then be displayed in FalconView.

HandHeld AWE	Connects Portable Flight Planning Software (PFPS) information to a hand-held Global Positioning System (GPS) receiver and vice versa.
RAT Suite	Displays the location of the start and end points of conflicts in FalconView.
TaskView	Provides electronic access to United States Message Text Format (USMTF) Air Tasking Order/Confirmation (ATOCONF), Air Tasking Order (ATO), and Airspace Control Orders (ACO).
TOLD	Computes takeoff, landing, and emergency landing data for most USAF and applicable Navy aircraft.
UbuildWiz	Creates a custom built aircraft for the Portable Flight Planning Software (PFPS).
Winder	Provides wind and temperature data to PFPS aircraft routes.
WinFpm	Accesses the digtized model of aircraft performance tech order data.
Repeat	
SeaCOM	Provides driver support for DAGR devices.
SLAP	Provides astronomical data.
Talon Host Software	Cryptographic unit
VideoScout	VideoScout® is a family of interoperable video exploitation and management systems to capture video and telemetry from a wide variety of Unmanned Aerial Vehicles (UAVs), receivers, sensors and INTEL network feeds.

Table 13. JTCW software (MARCORSYSCOM, 2014).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. APPROXIMATE FUEL CONSUMPTION FOR DIESEL GENERATORS

This chart approximates the fuel consumption of a diesel generator, based on the size of the generator and the load at which the generator is operating.

Generator Size (kW)	1/4 Load (gal/hr)	1/2 Load (gal/hr)	3/4 Load (gal/hr)	Full Load (gal/hr)
20	0.6	0.9	1.3	1.6
30	1.3	1.8	2.4	2.9
40	1.6	2.3	3.2	4.0
60	1.8	2.9	3.8	4.8
75	2.4	3.4	4.6	6.1
100	2.6	4.1	5.8	7.4
125	3.1	5.0	7.1	9.1
135	3.3	5.4	7.6	9.8
150	3.6	5.9	8.4	10.9
175	4.1	6.8	9.7	12.7
200	4.7	7.7	11.0	14.4
230	5.3	8.8	12.5	16.6
250	5.7	9.5	13.6	18.0
300	6.8	11.3	16.1	21.5
350	7.9	13.1	18.7	25.1
400	8.9	14.9	21.3	28.6
500	11.0	18.5	26.4	35.7
600	13.2	22.0	31.5	42.8
750	16.3	27.4	39.3	53.4
1000	21.6	36.4	52.1	71.1
1250	26.9	45.3	65.0	88.8
1500	32.2	54.3	77.8	106.5
1750	37.5	63.2	90.7	124.2
2000	42.8	72.2	103.5	141.9
2250	48.1	81.1	116.4	159.6

Table 14. Approximate Fuel Consumption of a Diesel Generator.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G. CAPSET IV TECHNICAL CHARACTERISTICS

Below is a chart depicting the characteristics of a CAPSET IV, according to TM 2000-OD/2C.

TECHNICAL CHARACTERISTICS

Transport	Truck, rail, ship, aircraft or helicopter		
Power Requirements	120/208 VAC, 60 Hz, 3-phase		
Size and Weight	(GETT)	Operational Trailer (OT)	Supplemental Equipment (SEIII)
Weight	4,165 lb.	4,196 lb.	3,620 lb.
Weight (Tongue)	348 lb.	376 lb.	N/A
Length	160 in.	132 in.	N/A
Width	86 in.	86 in.	N/A
Height	72 in.	86 in.	N/A
Square	95.6 sq. ft.	78.8 sq. ft.	N/A
Cube	573.4 cu. ft.	565 cu. ft.	331 cu. ft.

NOTE

"SE" denotes "supplemental equipment": components not transported on either the OT or GETT, but are transported in the HMMWV, or other vehicle, at unit discretion.

Table 15. Characteristics of a CAPSET IV, according to TM 2000-OD/2C.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX H. EXPERIMENTAL DATA

The raw measurements of all experiments conducted on the EOC-2 are presented below.

Date & Time In Hours	Minimum Watts	Date & Time In Hours	Average Watts	Date & Time In Hours	Maximum Watts
5/02/2014 10:00 AM - 5/02/2014 11:00 AM	159	5/02/2014 10:00 AM - 5/02/2014 11:00 AM	166.5	5/02/2014 10:00 AM - 5/02/2014 11:00 AM	174
5/02/2014 11:00 AM - 5/02/2014 12:00 PM	159	5/02/2014 11:00 AM - 5/02/2014 12:00 PM	185.833	5/02/2014 11:00 AM - 5/02/2014 12:00 PM	208
5/02/2014 12:00 PM - 5/02/2014 01:00 PM	159	5/02/2014 12:00 PM - 5/02/2014 01:00 PM	187.333	5/02/2014 12:00 PM - 5/02/2014 01:00 PM	218
5/02/2014 01:00 PM - 5/02/2014 02:00 PM	159	5/02/2014 01:00 PM - 5/02/2014 02:00 PM	171.833	5/02/2014 01:00 PM - 5/02/2014 02:00 PM	182
5/02/2014 02:00 PM - 5/02/2014 03:00 PM	152	5/02/2014 02:00 PM - 5/02/2014 03:00 PM	170.143	5/02/2014 02:00 PM - 5/02/2014 03:00 PM	190
5/02/2014 03:00 PM - 5/02/2014 04:00 PM	159	5/02/2014 03:00 PM - 5/02/2014 04:00 PM	174.667	5/02/2014 03:00 PM - 5/02/2014 04:00 PM	199
5/02/2014 04:00 PM - 5/02/2014 05:00 PM	182	5/02/2014 04:00 PM - 5/02/2014 05:00 PM	199.167	5/02/2014 04:00 PM - 5/02/2014 05:00 PM	208
5/02/2014 05:00 PM - 5/02/2014 06:00 PM	199	5/02/2014 05:00 PM - 5/02/2014 06:00 PM	211.5	5/02/2014 05:00 PM - 5/02/2014 06:00 PM	218
5/02/2014 06:00 PM - 5/02/2014 07:00 PM	199	5/02/2014 06:00 PM - 5/02/2014 07:00 PM	206.667	5/02/2014 06:00 PM - 5/02/2014 07:00 PM	218
5/02/2014 07:00 PM - 5/02/2014 08:00 PM	174	5/02/2014 07:00 PM - 5/02/2014 08:00 PM	183.667	5/02/2014 07:00 PM - 5/02/2014 08:00 PM	199
5/02/2014 08:00 PM - 5/02/2014 09:00 PM	174	5/02/2014 08:00 PM - 5/02/2014 09:00 PM	183.5	5/02/2014 08:00 PM - 5/02/2014 09:00 PM	199
5/02/2014 09:00 PM - 5/02/2014 10:00 PM	174	5/02/2014 09:00 PM - 5/02/2014 10:00 PM	184.667	5/02/2014 09:00 PM - 5/02/2014 10:00 PM	190
5/02/2014 10:00 PM - 5/02/2014 11:00 PM	167	5/02/2014 10:00 PM - 5/02/2014 11:00 PM	172	5/02/2014 10:00 PM - 5/02/2014 11:00 PM	190
5/02/2014 11:00 PM - 5/03/2014 12:00 AM	174	5/02/2014 11:00 PM - 5/03/2014 12:00 AM	174	5/02/2014 11:00 PM - 5/03/2014 12:00 AM	174
5/03/2014 12:00 AM - 5/03/2014 01:00 AM	167	5/03/2014 12:00 AM - 5/03/2014 01:00 AM	179.5	5/03/2014 12:00 AM - 5/03/2014 01:00 AM	190
5/03/2014 01:00 AM - 5/03/2014 02:00 AM	174	5/03/2014 01:00 AM - 5/03/2014 02:00 AM	183.333	5/03/2014 01:00 AM - 5/03/2014 02:00 AM	190
5/03/2014 02:00 AM - 5/03/2014 03:00 AM	167	5/03/2014 02:00 AM - 5/03/2014 03:00 AM	176.833	5/03/2014 02:00 AM - 5/03/2014 03:00 AM	190
5/03/2014 03:00 AM - 5/03/2014 04:00 AM	174	5/03/2014 03:00 AM - 5/03/2014 04:00 AM	180.667	5/03/2014 03:00 AM - 5/03/2014 04:00 AM	182
5/03/2014 04:00 AM - 5/03/2014 05:00 AM	174	5/03/2014 04:00 AM - 5/03/2014 05:00 AM	178	5/03/2014 04:00 AM - 5/03/2014 05:00 AM	182
5/03/2014 05:00 AM - 5/03/2014 06:00 AM	174	5/03/2014 05:00 AM - 5/03/2014 06:00 AM	176.667	5/03/2014 05:00 AM - 5/03/2014 06:00 AM	182
5/03/2014 06:00 AM - 5/03/2014 07:00 AM	167	5/03/2014 06:00 AM - 5/03/2014 07:00 AM	174.167	5/03/2014 06:00 AM - 5/03/2014 07:00 AM	182
5/03/2014 07:00 AM - 5/03/2014 08:00 AM	167	5/03/2014 07:00 AM - 5/03/2014 08:00 AM	168.167	5/03/2014 07:00 AM - 5/03/2014 08:00 AM	174
5/03/2014 08:00 AM - 5/03/2014 09:00 AM	167	5/03/2014 08:00 AM - 5/03/2014 09:00 AM	170.5	5/03/2014 08:00 AM - 5/03/2014 09:00 AM	174
5/03/2014 09:00 AM - 5/03/2014 10:00 AM	167	5/03/2014 09:00 AM - 5/03/2014 10:00 AM	172.8	5/03/2014 09:00 AM - 5/03/2014 10:00 AM	182
5/03/2014 10:00 AM - 5/03/2014 11:00 AM	167	5/03/2014 10:00 AM - 5/03/2014 11:00 AM	169.333	5/03/2014 10:00 AM - 5/03/2014 11:00 AM	174
5/03/2014 11:00 AM - 5/03/2014 12:00 PM	167	5/03/2014 11:00 AM - 5/03/2014 12:00 PM	169.333	5/03/2014 11:00 AM - 5/03/2014 12:00 PM	174
5/03/2014 12:00 PM - 5/03/2014 01:00 PM	167	5/03/2014 12:00 PM - 5/03/2014 01:00 PM	171.833	5/03/2014 12:00 PM - 5/03/2014 01:00 PM	182
5/03/2014 01:00 PM - 5/03/2014 02:00 PM	167	5/03/2014 01:00 PM - 5/03/2014 02:00 PM	175.5	5/03/2014 01:00 PM - 5/03/2014 02:00 PM	182
5/03/2014 02:00 PM - 5/03/2014 03:00 PM	167	5/03/2014 02:00 PM - 5/03/2014 03:00 PM	168.167	5/03/2014 02:00 PM - 5/03/2014 03:00 PM	174
5/03/2014 03:00 PM - 5/03/2014 04:00 PM	167	5/03/2014 03:00 PM - 5/03/2014 04:00 PM	169.333	5/03/2014 03:00 PM - 5/03/2014 04:00 PM	174
5/03/2014 04:00 PM - 5/03/2014 05:00 PM	167	5/03/2014 04:00 PM - 5/03/2014 05:00 PM	174.167	5/03/2014 04:00 PM - 5/03/2014 05:00 PM	182
5/03/2014 05:00 PM - 5/03/2014 06:00 PM	167	5/03/2014 05:00 PM - 5/03/2014 06:00 PM	169.333	5/03/2014 05:00 PM - 5/03/2014 06:00 PM	174
5/03/2014 06:00 PM - 5/03/2014 07:00 PM	167	5/03/2014 06:00 PM - 5/03/2014 07:00 PM	167	5/03/2014 06:00 PM - 5/03/2014 07:00 PM	167
5/03/2014 07:00 PM - 5/03/2014 08:00 PM	167	5/03/2014 07:00 PM - 5/03/2014 08:00 PM	170.5	5/03/2014 07:00 PM - 5/03/2014 08:00 PM	174
5/03/2014 08:00 PM - 5/03/2014 09:00 PM	167	5/03/2014 08:00 PM - 5/03/2014 09:00 PM	169.333	5/03/2014 08:00 PM - 5/03/2014 09:00 PM	174
5/03/2014 09:00 PM - 5/03/2014 10:00 PM	167	5/03/2014 09:00 PM - 5/03/2014 10:00 PM	169.333	5/03/2014 09:00 PM - 5/03/2014 10:00 PM	174
5/03/2014 10:00 PM - 5/03/2014 11:00 PM	167	5/03/2014 10:00 PM - 5/03/2014 11:00 PM	170.5	5/03/2014 10:00 PM - 5/03/2014 11:00 PM	174
5/03/2014 11:00 PM - 5/04/2014 12:00 AM	167	5/03/2014 11:00 PM - 5/04/2014 12:00 AM	169.333	5/03/2014 11:00 PM - 5/04/2014 12:00 AM	174
5/04/2014 12:00 AM - 5/04/2014 01:00 AM	167	5/04/2014 12:00 AM - 5/04/2014 01:00 AM	176.833	5/04/2014 12:00 AM - 5/04/2014 01:00 AM	182
5/04/2014 01:00 AM - 5/04/2014 02:00 AM	167	5/04/2014 01:00 AM - 5/04/2014 02:00 AM	175.667	5/04/2014 01:00 AM - 5/04/2014 02:00 AM	190
5/04/2014 02:00 AM - 5/04/2014 03:00 AM	167	5/04/2014 02:00 AM - 5/04/2014 03:00 AM	169.333	5/04/2014 02:00 AM - 5/04/2014 03:00 AM	174
5/04/2014 03:00 AM - 5/04/2014 04:00 AM	167	5/04/2014 03:00 AM - 5/04/2014 04:00 AM	170.5	5/04/2014 03:00 AM - 5/04/2014 04:00 AM	174
5/04/2014 04:00 AM - 5/04/2014 05:00 AM	174	5/04/2014 04:00 AM - 5/04/2014 05:00 AM	180.667	5/04/2014 04:00 AM - 5/04/2014 05:00 AM	190
5/04/2014 05:00 AM - 5/04/2014 06:00 AM	182	5/04/2014 05:00 AM - 5/04/2014 06:00 AM	182	5/04/2014 05:00 AM - 5/04/2014 06:00 AM	182
5/04/2014 06:00 AM - 5/04/2014 07:00 AM	182	5/04/2014 06:00 AM - 5/04/2014 07:00 AM	184.667	5/04/2014 06:00 AM - 5/04/2014 07:00 AM	190
5/04/2014 07:00 AM - 5/04/2014 08:00 AM	174	5/04/2014 07:00 AM - 5/04/2014 08:00 AM	176.667	5/04/2014 07:00 AM - 5/04/2014 08:00 AM	182
5/04/2014 08:00 AM - 5/04/2014 09:00 AM	182	5/04/2014 08:00 AM - 5/04/2014 09:00 AM	186	5/04/2014 08:00 AM - 5/04/2014 09:00 AM	190
5/04/2014 09:00 AM - 5/04/2014 10:00 AM	182	5/04/2014 09:00 AM - 5/04/2014 10:00 AM	184.667	5/04/2014 09:00 AM - 5/04/2014 10:00 AM	190
5/04/2014 10:00 AM - 5/04/2014 11:00 AM	174	5/04/2014 10:00 AM - 5/04/2014 11:00 AM	180.667	5/04/2014 10:00 AM - 5/04/2014 11:00 AM	182
5/04/2014 11:00 AM - 5/04/2014 12:00 PM	182	5/04/2014 11:00 AM - 5/04/2014 12:00 PM	186	5/04/2014 11:00 AM - 5/04/2014 12:00 PM	190
5/04/2014 12:00 PM - 5/04/2014 01:00 PM	182	5/04/2014 12:00 PM - 5/04/2014 01:00 PM	187.333	5/04/2014 12:00 PM - 5/04/2014 01:00 PM	190

Table 16. Raw Measurements of All Experiments Conducted on the EOC-2.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I. EOC-2 IDLE POWER DRAW

The screen shot below presents the idle power draw of the EOC-2 according to the systems Raritan PDU.

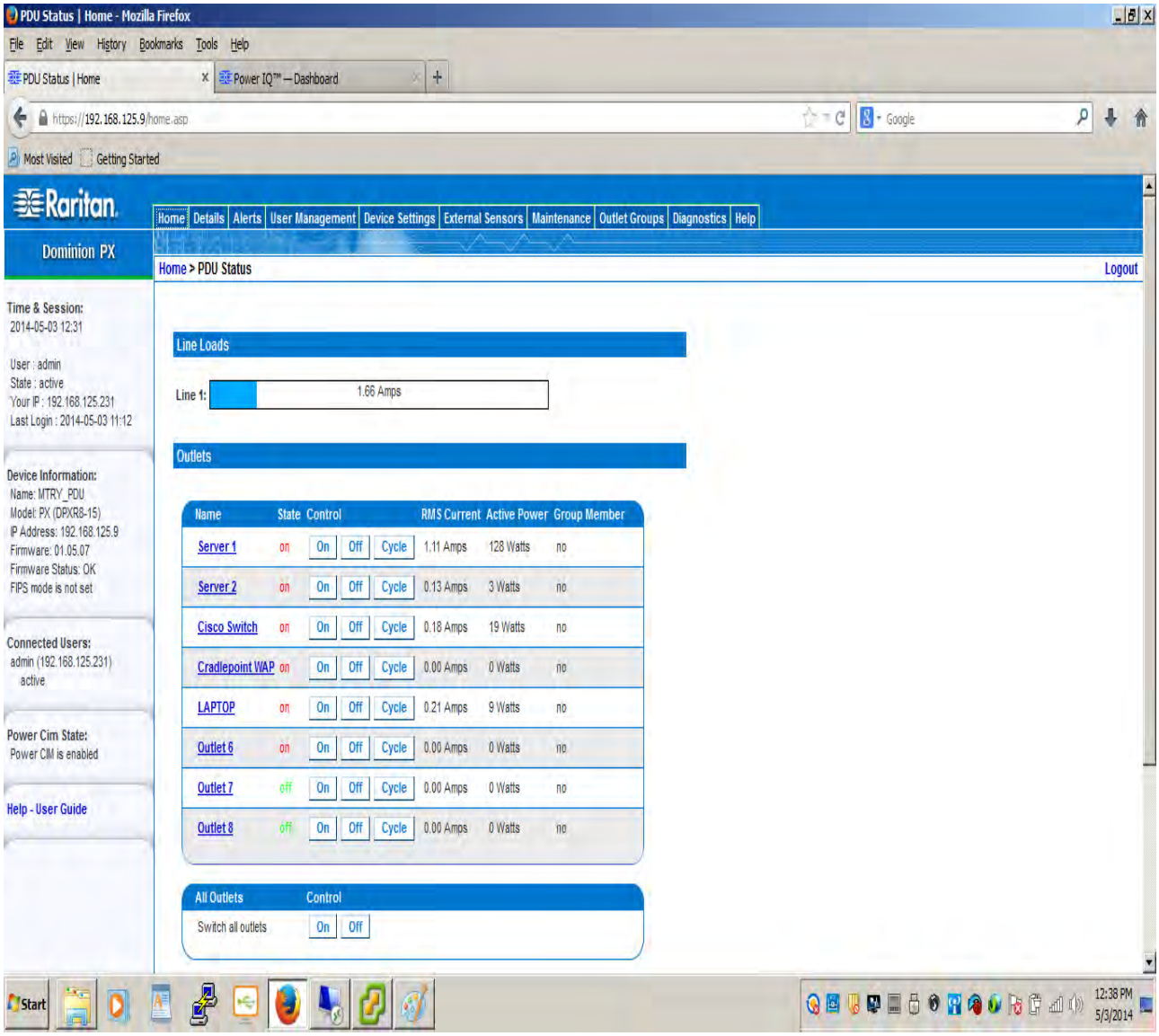

Figure 21. Idle Power Draw of the EOC-2

THIS PAGE LEFT INTENTIONALLY BLANK

LIST OF REFERENCES

Amos, J. A. (2010). *35th Commandant's planning guidance*. Washington, DC: U.S. Marine Corps. Retrieved from http://www.quantico.usmc.mil/uploads/files/CMC%2035%20Planning%20Guidance%20v.Q.pdf

Anderson, R. L. (2012). Marine Corps Private Computing Environment Strategy. Retrieved from http://fullnulled.com/doc/pdf/download/www__hqmc__marines__mil--Portals--156--Newsfeeds--SV%20Documents--Marine_Corps_Private_Cloud_Computing_Environment_Strategy_15_May_2012.pdf

Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. (1997). *DoD 5200.1-R: Information Security Program*. Washington, DC: Office of the Assistant Secretary of Defense.

Azab, A. M., Ning, P., Wang, Z., Jiang, X., Zhang, X., & Skalsky, N. C. (2010). Hypersentry: Enabling stealthy in-context measurement of hypervisor integrity. *Proceedings of the 17th* Association for Computing Machinery *Conference on Computer and Communications Security,* CCS 38–49.

Barreto A. (2011). *Integration of virtual machine technologies into Hastily Formed Networks in support of humanitarian relief and disaster recovery missions* (Master's thesis). Retrieved from http://calhoun.nps.edu/public/handle/10945/10736

Buyya, R., Yeo, C. S., & Venugopal, S. (2008). Market-oriented cloud computing: vision, hype, and reality for delivering it services as computing utilities, *10th Institute of Electrical and Electronics Engineers International Conference on High Performance Computing and Communications.*, pp.5–13. doi 10.1109/HPCC.2008.172

Combat Development and Integration. (2011). *Concept of employment for an infantry company and below* (ICB-C2). Washington, DC: Headquarters Marine Corps.

Corrin, A. (2011). DoD not ready for total cloud migration, CIO says. *FCW, The Business of Federal Technology*. Retrieved from http://few.com/articles/2011/04/21dod-cio-takai-acquisition-reform-cloud.aspx

Denning, P. J. (2006). Hastily Formed Networks. *Communications of the Association for Computing Machinery*, *49*(4),1–2.

Department of Defense. (2005). *Assistant Secretary of Defense for networks and information integration/DoD Chief Information Officer* (ASD(NII)/DoD CIO. Department of Defense Directive Number 5144.1. Washington, DC: Author.

English, J. T., & Nelson, G. S. (2010). Manual lifting: Historical sources of current standards regarding acceptable weights of lift. Texas Engineering Firm Reg. #F-006396. Retrieved from http://www.hazardcontrol.com/factsheets/ml-mh/evolution-of-manual-lifting-standards

Fulks, B. (2013). *Operator's manual for Mine Resistant Ambush Protected All Terrain Vehicle (M-ATV*) TM 11803A-OI. Washington, DC: U.S. Marine Corps. Retrieved from https://portal.logcom.usmc.mil/sites/pubs/500/50011803000.pdf

General Dynamics C4 Systems. (2011). Fortress ES820. Retrieved from http://www.gdc4s.com/es820?taxonomyCat=132

General Dynamics C4 Systems. (2002). Combat Operations Center capability set. Retrieved from http://www.gdc4s.com/combat-operations-center-(coc).html

Ghazisaeedi, E., Wang, N., & Tafazolli, R. (2012). Link sleeping optimization for green virtual network infrastructures. *2012 Institute of Electrical and Electronics Engineers Globecom Workshops (GC Wkshps),* (pp. 842–8460). doi: 10.1109/GLOCOMW.2012.6477685

Glenn W. Goodman, Jr. (2010). "S&T and Cost Estimating," in Scott R. Gourley (Ed.), *Nearly Four Years in Operation: Program Executive Officer Land Systems Marine Corps Looks Ahead to the Future*, Quantico, VA: Program Executive Office, Land Systems Marine Corps.

Grosch, H. (1953). High speed arithmetic: The digital computer as a research tool, J*ournal of the Optical Society of America, (43)*4, 306–310.

Hale, R. A., & Nicely, S. L. (2013). Committee on national security systems. Meeting current and future threats a message from the CNSS chair & co-chair. Retrieved from https://www.cnss.gov/CNSS/about/faq.cfm

Harris Secure Communications. (2013). SecNet 54 Radio Module (RMOD) Secure Wireless Local Area Network. Retrieved from http://rf.harris.com/media/SecNet54_tcm26-9221.pdf

Ibatuan II, C. R. (2013). *Cloud computing solutions for the Marine Corps: An architecture to support expeditionary logistics* (Master's thesis). Retrieved from http://calhoun.nps.edu/public/handle/10945/37643

iGov, (2013). Hardware modernization engineering change proposal [Press release]. Retrieved from http://www.igov.com/component/content/article/32-press-releases/146-igov-awarded-usmc-combat-operations-center-coc-modernization-contract-

Inmarsat. (2013). BGAN. Retrieved from http://www.inmarsat.com/services/bgan?OverrideCls=inmarsat:service_bganvehicular

Kelly, T. K., Peters, E. J., Landree, E., Moore, L. R., Steeb, R., & Martin, A. (2011). *The U.S. combat and tactical wheeled vehicle fleets: Issues and suggestions for Congress*. Santa Monica, CA: Rand.

Kessel, A., & Goodwin, S. (2005). *Wireless local area network (WLAN) vulnerability assessment and security.* (Master's thesis). Retrieved from http://calhoun.nps.edu/public/handle/10945/1939

Kubic, C. (2008). DoD cloud computing security challenges. Retrieved from http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008–12/cloud-Computing-IA-challenges_ISPAB-Dec2008_C-Kubic.pdf

Law, L., & Solinas, J. (2011). Internet Engineering Task Force. Suite B Cryptographic Suites for IPsec. Request for comments: 6379. ISSN: 2070-1721. Retrieved from https://tools.ietf.org/html/rfc6379

Lawlor, M. (2004). New operations centers set the stage for consistent technology acquisition. *Signal Online.* Retrieved from http://www.afcea.org/content/?q=node/217

Leavitt, N. (2009). Is cloud computing really ready for prime time?, *Computer*, *(42)*1, 15, 20

Liguori, M. A., & Daniel, N. Z. (2013). *Secure mobile cellular capabilities: Value analysis for expeditionary combat units*. (Master's thesis). Retrieved from http://calhoun.nps.edu/public/handle/10945

L3 Communication Corporation Systems-East. (2013). *Talon user manual*. Retrieved from http://www2.l-3com.com/cs-east/ia/talon/ie_ia_talon.shtml

Mandal, S. K., & Khilar, P. M. (2013). Efficient virtual machine placement for on-demand access to infrastructure resources in cloud computing. *International Journal of Computer Applications, 68*(12). doi: Retrieved from http://research.ijcaonline.org/volume68/number12/pxc3887101.pdf

Marine Corps. (2013). *America's Expeditionary Force in Readiness, Programs and Resources*. Washington DC: Author. Retrieved from http://www.hqmc.marines.mil/pandr/ConceptsandPrograms/ConceptsandPrograms2013.aspx

Marine Corps. (2012). *Science & Technology Strategic Plan. Leading edge technology for the Marines of tomorrow*. Washington, DC: U.S. Marine Corps. Retrieved from http://www.onr.navy.mil/~/media/Files/About-ONR/USMC-ST-Strat-Plan-2012-Final-31Jan.ashx

Marine Corps. (2008). *Marine Corps urgent needs statement* (Marine Corps Order 3900.17). Washington, DC: Author. Retrieved from

Marine Corps. (1996). *Doctrinal Publication (MCDP) 6. Command and Control.* Washington, DC: Author.

Marine Corps Systems Command. (2014). *Networking on-the-Move (NOTM), program overview*. Quantico VA: Author.

Marine Corps Systems Command. (2012). Program Executive Officer Land Systems. Retrieved from http://www.defenseinnovationmarketplace.mil/resources/MarineAirGroundTaskForceCommandControlCommunications.pdf

Marine Corps Technical Manual, TM 11033-OR. (2012). *Operator's manual for truck Utility*. U.S. Marine Corps. Washington, DC: U.S. Marine Corps. https://portal.logcom.usmc.mil/sites/pubs/184/18411033000.pdf

Marine Corps Technical Manual TM 2000-OD/2C. (2005). *Principal technical characteristics of U.S. Marine Corps communication-electronics equipment*. PCN 180 002310 00. Washington, DC: U.S. Marine Corps Retrieved from http://www.docstoc.com/docs/document-preview.aspx?doc_id=151146038

Marshburn, E. R. (2011). *Supporting command and control (C2) of an embarked commander: Tunneling SIPRNet data across an UNCLAS Wireless LAN.* (Master's thesis). Retrieved from http://calhoun.nps.edu/public/handle/10945/16/browse?value=Marshburn%2C+Erik+R.&type=author

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*, NIST Special Publication 800-145, Gaithersburg, MD: National Institute of Standards and Technology.

Military Battery Systems. (2014). Military Battery Systems [Fact sheet].Retrieved from http://www.milbatteries.com/images/stories/accessories/tt/april_14_nato_connectors_cables.pdf

Military Standard Human Engineering Design Criteria for Military Systems. (1989). Equipment and Facilities. Philadelphia, PA: Naval Publications and Forms Center

Nally, K. J. (2013). Director for Command, Control, Communications, and Computers (C4) and the Department of the Navy Deputy Chief Information Officer (2013). *Marine Corps commercial mobile device strategy*. Washington, DC: Author. Retrieved from http://fedne.ws/uploads/2014_APR_USMC_mobile_device_strategy.pdf

National Security Agency. (2009). Suite B cryptography – National Security Agency, Central Security Service. Washington DC. Retrieved from http://www.nsa.gov/ia/programs/suiteb_cryptography/

Oh, T., Lim, S., Choi, Y. B., & Ryoo, J. (2011). Security Implication in Virtualization. *Encyclopedia of Cryptography and Security*. New York: Springer.

Perez-Botero, D., Szefer, J., & Lee, R. B. (2013). Characterizing hypervisor vulnerabilities in cloud computing servers. *Proceedings of the Association for Computing Machinery Conference on Computer and Communications Security*, 3–10.

Perez, R., & van Door, L. (2008). Virtualization and hardware-based security. *Institute of Electrical and Electronics Engineers* Security Privacy 6(5): 24–31.

Postel, J. (1981). *Request for comment 791. Internet protocol. DARPA Internet program, protocol specification.* Retrieved from https://datatracker.ietf.org/doc/rfc791/?include_text=1

Ray, E., & Schultz, E. (2009). Virtualization security. *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies* (CSIIRW '09), Frederick Sheldon, Greg Peterson, Axel Krings, Robert Abercrombie, and Ali Mili (Eds.), 5.

Regalado, A. (2011). :Who coined “cloud computing?. *MIT Technology Review*. Retrieved from http://goo.gl/m4stls.

Ryan, P.S., Falvey, S., & Merchant, R. (2013). When the cloud goes local: the global problem with data localization, *Computer*, *(46)*12, 54, 59.

Scarfone, K., Souppaya, M., & Hoffman, P. (2011). *Guide to security for full virtualization technologies.* NIST Special Publication 800-125. Gaithersburg, MD:National Institute of Standards and Technology.

Sharp, M., Rosenberger, M., & Knapik, J. (2009). Optimizing operational physical fitness. Retrieved from http://www.cism-milsport.org/eng/004_SPORT_AND_SCIENCE/articles-and-pdfs/018-NATO-HFM-080_Final_Report_Jan_09.pdf

Smith, J. E., & Nair, R. (2005). The architecture of virtual machines. *Computer, 38*(5), 32–38. Retrieved from http://search.proquest.com/docview/197407972?accountid=12702

Szefer, J., Keller, E., Lee, R. B., & Rexford, J. (2011). Eliminating the hypervisor attack surface for a more secure cloud. Princeton, NJ: Princeton University.

Techopedia. (2014). Air gap. Retrieved from http://www.techopedia.com/definition/17037/air-gap

Testing Anywhere. (2014). Server testing software. Retrieved from http://www.automationanywhere.com/Testing/?r=google&w=testinganywhere&kw=Testing%20Anywhere&match=p&network=g&place=&gclid=CLmZ0IS4_L0CFYqIfgodAooAsg

United States Department of Labor, Occupational Safety & Health Administration. (2014). Materials handling: Heavy lifting. Retrieved from https://www.osha.gov/SLTC/etools/electricalcontractors/materials/heavy.html

United States Government Accountability Office. (2010). *Information security, federal guidance needed to address control issues with implementing cloud computing* (GAO-10513). Washington, DC: Author. Retrieved from http://www.gao.gov/assets/310/305000.pdf

van Cleeff, A., Pieters, W., & Wieringa, R. (2009). Security implications of virtualization: A literature study, *CSE 2009, International Conference on Computational Science and Engin*eering *2009: Vol. 4*. (pp. 353, 358).

Venkatesh, R., Otis, A. J., & Bretl, R. F. (2001). Transactional virtual machine architecture. United States patent number US 6,256,637 B1.

Wikitravel. (2013). Commercial airline baggage limitations. Retrieved from http://wikitravel.org/en/Airline_baggage

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California